Time for Improvement

The 1986 UN Remote Sensing Principles in the Information Age

Stefan A. Kaiser[*]

Abstract

Thirty years after the UN General Assembly's adoption of the Principles Relating to Remote Sensing of the Earth from Outer Space, the technical, organisational and societal context of Earth observation, information analysis and distribution has dramatically changed. Information technology is broadly available in many parts of the world. Analysed information is generated not only by governmental bodies, but also by private value added service providers detached from the operation of remote sensing space systems, primary data collection and storage stations. The manifold sources of analysed information and their broad dissemination in the information age have therefore developed their own dynamics. Territorial sovereignty is today not such a limiting factor as perceived in the time, when the UN Remote Sensing Principles were drafted. In commercial applications, value added non-space derived content becomes a stronger driver than primary and processed data. The broad use of such non-space derived content stimulates the demand for primary data with higher resolution, more frequent updates and, in the future, even permanent viewing. Moreover, the UN Remote Sensing Principles do not consider the linking of remote sensing and personal information and the related privacy implications, the use of remote sensing for (national) law enforcement and the connection between remote sensing and (satellite) navigation. This article explores the gaps of the UN Remote Sensing Principles and areas which may need a review in light of the technical and societal changes during the last thirty years.

I. Introduction

The UN Remote Sensing Principles[1] are a product of their time. Adopted by resolution of the United Nations General Assembly in 1986, the Remote

* LLM (McGill). Wassenberg, Germany, stefanakaiser@aol.com.

Stefan A. Kaiser, 'Time for Improvement: The 1986 UN Remote Sensing Principles in the Information Age' Proceedings of the 59th Colloquium on the Law of Outer Space (2016).

Sensing Principles followed the "golden age of space law" from 1967 until 1979, when the five space treaties were signed. After the moon race was over, the United States of America and the then Soviet Union had lost interest in committing to hard international treaty law for space affairs. However, the momentum of other States, most notably those represented in the UN Committee on the Peaceful Uses of Outer Space (COPUOS), who desired to establish more comprehensive space regulations, led to the establishment of sets of principles intended to cover the gaps not covered by the five treaties. As a UNGA resolution, the Remote Sensing Principles, just like the principles on direct broadcasting (1982)[2] and on nuclear power sources (1992),[3] are thus non-binding recommendations. Having been negotiated and drafted in UNCOPUOS for about two decades, the Remote Sensing Principles are a product of compromise and hardly offer substantive innovations. Many of the concepts are re-statements or implementations of existing principles of the Outer Space Treaty[4] or the other space law treaties, for example the principle for the benefit and in the interest of all countries,[5] accordance with international law,[6] the promotion of international cooperation,[7] registration[8] and responsibility.[9]

Understanding the UN Remote Sensing Principles requires a closer look at the areas *not* covered and at the conflicting views expressed during the negotiations. Important topics are left out or masked by compromise. For example, the military and security uses of remote sensing did not find their way into the UN Remote Sensing Principles. Also, the debate about the prior consent concept of the sensed State – finally rejected – left some traces in the text.

1 Principles relating to remote sensing of the Earth from outer space, UNGA Res. 41/65, 3 December 1986.
2 Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting, UNGA Res. 37/92, 10 December 1982.
3 Principles Relevant to the Use of Nuclear Power Sources in Outer Space, UNGA Res. 47/68, 14 December 1992.
4 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 27 January 1967, 610 U.N.T.S. 205.
5 Principles II and IV re-stating and implementing Article I.1 of the Outer Space Treaty.
6 Principle III re-stating Articles 1.2 and 3 of the Outer Space Treaty.
7 Principles V and VIII re-stating and implementing Articles I, III, IX, XI of the Outer Space Treaty.
8 Principle IX referring to Article IV of the Convention on Registration of Objects Launched into Outer Space (1974), 1023 UNTS 15.
9 Principle XIV about international responsibility referring to Article VI of the Outer Space Treaty.

II. Military and Security Uses of Remote Sensing

The Remote Sensing Principles do not apply to military, security and law enforcement uses of remote sensing. Even though it may not be surprising that the negotiating States limited the Remote Sensing Principles to certain civilian uses and deliberately excluded the difficult area of military and security uses, it should be remembered that – military – remote sensing was the first space application ever. It is not a secret that from the beginning of the space age, the United States of America and the Soviet Union used satellites for military remotes sensing, today also referred to as intelligence, surveillance and reconnaissance (ISR). These clandestine activities of the two superpowers were officially declared as research activities,[10] but mutually acquiesced as an accepted form of observation. This laid the foundation for an international practice of all other States. In essence it means that the freedom of the exploration and use of outer space includes any kind of space based remote sensing of the Earth. The Remote Sensing Principles are silent on military and security operations, which is in contrast to the Outer Space Treaty, whose scope is not limited to civilian applications.

Drawing the dividing line between military and security versus civilian and commercial uses of remote sensing can be difficult. The resolution of the images is commonly used as a tool. Higher resolution images are reserved for military and security purposes and *not* distributed for civilian and commercial uses and for export. During the negotiations, the Soviet Union proposed, without success, to introduce spatial resolution as a parameter, so that the distribution of imagery with a resolution of less than 50 metres would have required the approval of the sensed State.[11] It is clear that a fixed delimitation of the resolution would have been counter-productive, since any fixed value has been gradually changing with the evolving state of technology. National remote sensing data policies have thus used spatial resolution as a *relative* parameter to release imagery for civil, commercial and export purposes.[12] This means, seen over longer periods, national data polices

10 About US. and Soviet spy satellites disguised as research programs see Bill Yenne, Secret Weapons of the Cold War, Berkley Publishing Group, New York, 2005, at chapter 2.

11 UN Doc. A/AC.105/240, Annex I, Appendix B, 10 April 1979.

12 See for example, United States of America: Land Remote Sensing Policy Act, 15 U.S.C. § § 5601-5672 (1992), U.S. Commercial Remote Sensing Policy, 25 April 2003, www.whitehouse.gov/files/documents/ostp/press_release_files/fact_sheet_commercial_remote_sensing_policy_april_25_2003.pdf; European Union: Regulation (EU) No 1159/2013 of 12 July 2013 … on the European Earth monitoring programme (GMES) by establishing registration and licensing conditions for GMES users and defining criteria for restricting access to GMES dedicated data and GMES service information; France: LOI n° 2008-518 du 3 juin 2008 relative aux opérations spatiales, especially Art. 23; Germany: Satellitendatensicherheitsgesetz (SatDSiG) and Satellitendatensicherheitsverordnung (SatDSiV).

have authorized, step-by-step, higher spatial resolutions for the distribution of images for civilian and commercial purposes. Other limitations of national data policies are spectral,[13] temporal[14] and geographical[15] parameters. Also, the export of data and information to critical destinations are limited by national remote sensing or data distribution policies. All such parameters which define security critical red-lines cannot be found in the Remote Sensing Principles, which pretend that specified civilian and commercial uses are completely detached from military and security aspects.

III. The Limited Purpose of the Remote Sensing Principles

Principle I (a) has a very narrowly defined purpose listing only "improving of natural resource management, land use and the protection of the environment."[16] For most of the text, the Remote Sensing Principles avoid references to specific purposes. However, besides Principle I (a), also Principles X and XI need to be mentioned. Principle X requires States to disclose information "that can be used to avert any phenomenon harmful to the Earth's natural environment". Under principle XI States shall transmit data and information useful to protect mankind from natural disasters.[17]
30 years after the adoption of the Remote Sensing Principles, Principles X and XI can be considered as having become the foundations for more elaborate international programs and arrangements on disaster relief and environmental protection. To that end, the exchange of data and information among national and multinational operators of meteorological and environmental satellites are an everyday reality. The distribution of information relevant for handling disasters is facilitated by the United Nations' Space-based Information for Disaster Management and Emergency Response (UN Spider), a co-operation under the so-called international charter on space and disaster relief among agencies operating Earth remote sensing satellites.[18]

---

13 The spatial resolution may differ depending on different wavelengths of the electromagnetic spectrum.

14 Time limitations are to avoid the distribution of up to date images that would allow the monitoring of security activities or personal movements.

15 For security reasons and for considerations of foreign policy, States restrict remote sensing of security sensitive locations and countries, typically referred to as "shutter control."

16 It must be noted that the purpose clause defines remote sensing in this narrow way, as if remote sensing activities for other purposes do not constitute remote sensing. This is apparently misleading and should rather mean that remote sensing for other purposes are not governed by the Remote Sensing Principles.

17 It also must be noted that the protection of mankind from natural disasters is not covered by the definition of Principle I (a) and can thus be misconstrued as to fall outside of the purpose of the Remote Sensing Principles as such!

18 http://www.un-spider.org/.

IV. The Impact of Sovereignty on the Remote Sensing Principles

During the negotiations of the Remotes Sensing principles some States supported the concept that remote sensing of the Earth from outer space had to be subject to the prior consent of the sensed state.[19] Connected to this issue was the debate, whether access to data and information should be restricted[20] or unrestricted.[21] Finally, the prior consent concept of the sensed State was rejected and an unrestricted regime for dissemination of data and information was adopted,[22] both of which shaped Principles IV and XII. Under Principle IV, remote sensing "shall be conducted on the basis of respect for the principle of full and permanent sovereignty of all States and peoples over their own wealth … and shall not be conducted in a manner detrimental to the legitimate rights and interests of the sensed State." How this is to be achieved can be read in Principle XII. The sensed State shall have access to "the primary and processed data" of its territory "on a non-discriminatory basis and on reasonable cost terms …" and also "… to the available analysed information concerning the territory under its jurisdiction …on the same basis and terms …".

Principle IV establishes a relationship between remote sensing and sovereignty, which is unprecedented in other space law documents. The Outer Space Treaty does not use sovereignty in a comparable context.[23] Starting point of Principle IV is the sovereignty over natural resources, which is an undisputed concept. Principle XII is used as leverage for the right of access to images, data and information of its territory. As Principle IV shows, this leverage is rooted in the sovereignty over national wealth and natural resources, not in national security, which is outside of the scope of the Remote Sensing Principles. Using sovereignty as an argument for access to data and enhancements is a paradigm shift. When Principle IV mentions that the exploration and use of outer space shall be carried out for the benefit and in the interest of all countries, in the context of Principle XII it expands this concept from actual space activities to the products derived therefrom: images and data. Another important stepping stone for this paradigm shift can be found in the definitions of Principle I (b), (c),

19 See for example Art. V of the draft "Treaty on Remote Sensing of Natural Resources by Means of Space Technology" by Argentina and Brazil, UN Doc. A/C.1/1047, 15 October 1974.

20 See proposal of Argentina and Brazil, *ibid*, and of France and the Soviet Union, UN Doc. A/AC.105/C.2/L.99 27 May 1974.

21 See proposal of the U.S.A., UN Doc. A/AC.105/C.2/L.103, 19 February 1975.

22 For more details on this issue see Ivan Vlasic, Remote Sensing of the Earth by Satellites, in Nandasiri Jasentuliyana, Roy S. K. Lee (eds.), Manual on Space Law, volume I, 1979, Oceana Publications, New York, at pp 319-321.

23 Article II of the Outer Space Treaty rather states that outer space is *not* subject to national appropriation by claim of sovereignty.

(d), which define "primary data", "processed data" and "analysed information". These definitions set the scene for Principles that have their centre of gravity more on data and information than on the actual space activities as such.

V. The Remote Sensing Principles in the Information Age

This conceptual shift from a space activity to the use and distribution of data and information is the link to the information age. The information age is characterized by an information based society and commerce with global information exchanges over computer networks. It has changed our lives during the last two decades, like the industrial revolution in the 19th century changed society. And that is the aspect the Remote Sensing Principles could not capture in 1986.

Knowing today's information industry, it can be said that the importance has swung from primary data to analysed information. In 1986 it was already understood that from the end-user perspective analysed information is a more valuable product than primary data, because it is the final product which can be directly used for various applications. For that reason, Principle I distinguishes between "primary data" as the "raw data … acquired by remote sensors by a space object and that are transmitted … to the ground" and "analysed information" as the result of "the interpretation of … data, inputs of data and knowledge from other sources".[24] However, it was also clear that any analysis or interpretation is only possible, if there are primary data as the basic product.

As we understand today's information industry, the manifold sources of analysed information, their broad dissemination and an increasing number of value enhancing service providers have developed their own dynamics. In these environments, value added non-space derived content becomes a stronger driver than primary and processed data. Not only that. The broad use of non-space derived content stimulates the demand for primary data with higher resolution, more frequent updates and, in the future, even permanent viewing.

In the information age, data and information can flow more freely and broadly and the number of players increases. In 1986 no one thought of massive global flows of data over the internet, accessible to almost everybody

24 Principle I (c) also defines "processed data" as "the products resulting from the processing of the primary data, needed to make such data usable". This type of data is a product of technical processing, without any added value to the content of the data. It reflects only a technical step of processing dependent on the technology used for the remote sensing activity. For example, photographic film – today not used any longer for space based remote sensing – needs to be chemically developed, after which it qualifies as processed data.

in developed countries. Likewise, no one foresaw problems of cross border jurisdiction and enforcement in regard to data streams, of privacy and intellectual property protection, the impact on national and international security or even cyber security. When the Remote Sensing Principles were adopted, the distribution of data and information in electronic formats were conceived to be a matter of States, research organisations and multi-national companies, not of small businesses or even individuals. The drafters of the Remote Sensing Principles were concerned that space faring nations could monopolize remote sensing data and information. Today these worries are not any longer an issue. The role of private organisations, who are not operators of satellites or ground segments, is steadily increasing. They provide value added information services worldwide and use all kinds of information from manifold sources, one of which can be data derived from space activities. This is the result of national policies to commercialize remote sensing, with the Landsat System[25] in the United States and Spot Image[26] in France as forerunners. Also, the international exchange of meteorological data and information, including the creation and operation of EUMETSAT,[27] an international governmental organisation in that field, has contributed to abundantly available, up-to-date products, hardly imagined of in 1986.

Today remote sensing is not any more limited to the observation of natural resources and the environment, but a value-added service industry is creating new products with an increasing information content from other sources, as compared to the primary data it is based on. The systems to collect, store, analyse and manage these data with reference to locations are also called geographical information systems (GIS). New information products require updated primary data, if possible instantly, which is therefore one of the areas where national data policies set limits. To understand the practical implications, we need to look at the various sources of data and information, apart from space remote sensing, and their informational linkage in geolocation:

(a) *In situ collection* of data and information may at first glance look harmless. For example, everybody may see that a vehicle is parked in front of a house at a certain moment and take a photo if this scene. From a privacy perspective, it gets critical, when *in situ* information is gathered in a systematic, automated and repetitive manner. Permanently installed webcams and private programs like "Google Street View" are such mechanisms. The same applies to photos and information privately taken by individuals with their smart-phones who upload them on the internet without considering the privacy of

25 See also the Land Remote Sensing Policy Act, *supra* footnote 12.

26 See also *supra* footnote 12.

27 See also the EUMETSAT Data Policy of July 2016, https://www.eumetsat.int/cs/groups/public/documents/document/dgff/cg9s/~edisp/pdf_leg_data_policy.pdf.

others. A more recent method of taking photos and measurements is by drones, many of them operated by private persons as a hobby.[28]

(b) Also the *virtual collection* of data and information over the internet can be critical. The virtual collection may not always happen with the consent of the owner or it may occur under terms and conditions that have a privacy impact a normal user can hardly comprehend. The virtual collection of information is an industry, often referred to as "data mining". It bears the risk that information created for virtual use may not be correct and, without being verified, can be multiplied and create a wrong image of, or even harm to, an individual.

(c) The *location nexus* is the key of geolocation and navigation. Data and information, however collected, can be attributed to a location, like a house or a business. Geolocation functionalities can be hidden in internet features that private users, including minors, are not aware of and may agree to, without understanding the implications, for example when playing the internet game "PokemonGo".[29] The location nexus is an important step in individualizing information and assigning it to a natural or legal person. A vast new area for these evolving information products is the combination with *navigation*. End user units for satellite navigation are constantly enhanced by increasingly refined data-bases that create the nexus between geographical locations and manifold other information. In this way, satellite navigation services have evolved into an *in-situ* application of information products that are derived, directly or indirectly, from remote sensing.

(d) The *timing element* becomes crucial, when data and information are constantly updated or made available in real-time. The activities of persons and businesses, but also of governments and law enforcement agencies can thus be followed on a permanent basis. The result cannot only be portrayed as transparency, but it can lead to stalking, industrial espionage and undermine the work of the military and law enforcement agencies.

(e) *Linking and administering information* is the central element in connecting the information gathered remotely, *in situ* and virtually. Traditionally, electronic information has been linked in data bases

28 Imaging from drones is in the strict sense not a collection of information *in situ*, but remote sensing, albeit from a much shorter distance than space remote sensing. Other than space remote sensing, the taking of images from aircraft and drones can be restricted and prohibited by the overflown State in accordance with Article 36 of the Convention on International Civil Aviation, 7 December 1944, 15 U.N.T.S. 295.

29 "Pokémon Go" is a tool to reveal geo-locating data and photographs to the developer/operator of the game by activating the navigation and camera function of the player's smart-phone.

administered by a person or organization, who is subject to the applicable national data protection rules. Today millions of smart phone users daily contribute data and information through social networks. The social networks arrange and link the data and information in accordance with criteria like geolocation or persons. Automated processes like voice and face recognition[30] enhance the linking, *identification and authentication.*

(f) *Electronic distribution* of data and information over international networks like the internet remains another big issue. In 1986 it was not foreseen that huge portions of the global population would have direct access to digital information. So far, States abstain from accepting responsibility for activities on international data networks. Identifying the proper jurisdiction for information of constantly re-routed cross-border data flows is a practical problem. In addition, States are reluctant to undertake enforcement measures in that arena.

(g) New technologies go a step further by linking, administering and distributing information in *integrated systems*. This may be achieved not only on the ground, but also by new *mega satellite low earth orbit constellations* for high-speed internet, which are to provide the fifth generation (5G) wireless infrastructure.[31] 5G networks will include the capability for wireless sensor networks, which means monitoring and surveillance of physical aspects over a network consisting of hundreds, possibly thousands of low earth satellites and drones. This means that 5G networks will not only provide communication connectivity like the internet, but also combine remote sensing capabilities, geolocation and automated signal intelligence for identification and authentication.

What does all that imply in terms of policy and law? In the information age, the focus is not any longer on the prevention of monopolies for remote sensing and space derived data, but it must be on the prevention of monopolies for geolocation information in general and on an internationally uniform protection against the misuse of data. This can already be seen in the various national policies on space remote sensing, which on one hand may foster the distribution and commercialisation of data, but on the other establish safeguards for national security and foreign policy. In addition, we see new critical areas that need protection as a result of the increasing spatial resolution and a plethora of information from other sources.

30 See also Luke Dormehl, Facial recognition: is the technology taking away your identity?, The Observer, 04 May 2014, https://www.theguardian.com/technology/2014/may/04/facial-recognition-technology-identity-tesco-ethical-issues.

31 See for example Jono Anderson, The Coming Satellite Revolution, AW&ST 15-28 August 2016, p. 58.

These shortcomings are not specific to remote sensing or space policy and law, but they relate to the global information industry and need to be tackled in a broader context. Despite existing national legislation on personal privacy and data protection, on the protection of intellectual property and, of course, on the protection of their national and international security, the practical developments of geolocation make it increasingly difficult to warrant an effective protection. Moreover, the understanding and application of rules on the protection of privacy and intellectual property differ from country to country and related practices are internationally not uniform.

VI. Conclusion

In 1986 the Remote Sensing Principles did not offer innovations on the field of space law, but they established principles for international data distribution at a time, when cross border data flow was only about to emerge. Ahead of their time, the Remote Sensing Principles do not address today's pertinent problems. By limiting their purpose to remote sensing of natural resources and the environment and by promoting the distribution of data, the Remote Sensing Principles have a blind spot on privacy, intellectual and industrial property and on the sensitive demarcation between the free flow of information and security interests.

Nevertheless, one can say the 1986 Remote Sensing Principles have achieved their purpose, because they clarified that the remote sensing from space is permissible without prior consent of the sensed State and because they laid the ground for numerous arrangements on the cooperation in data exchange and sharing. However, the Remote Sensing Principles are too focused on sovereignty over natural resources and too narrow to cope with the problems of the information age. The proportion of information in geographical information systems which is derived from space remote sensing becomes increasingly smaller. Also, the borders between remote sensing by satellite and by drone will increasingly blur.

(a) Considering all the mentioned developments of the information age, it does not appear meaningful to elaborate or update the Remote Sensing Principles.

(b) States need to take a broader approach on the protection of privacy, intellectual property and national and international security in the information age, rather than only for space remote sensing data and information. This could be possible within the framework of the United Nations.

(c) Policy and law makers need to critically monitor technical developments of satellite systems, which *integrate* remote sensing, communication connectivity like the internet, geolocation, navigation and automated signal intelligence for identification and authentication. Mega satellite constellations for 5G wireless

connectivity will be such integrated systems and also embed remote sensing. The future challenges will not only be remote sensing systems with higher spatial resolution and spectral capabilities, but the space based integration of all technical features of the information age on a global scale with unprecedented "data mining" potential. Therefore, future principles or regulations must address space remote sensing not as an isolated functionality, but the entire integrated capabilities as we see them emerge in the 5G wireless context.

(d) Informational monopolies of such integrated systems must be prevented. Privacy, intellectual property and national and international security must be safeguarded for such space based integrated systems, if possible, by a new international regime.

(e) Even though national rules on the protection of privacy and intellectual property exist, practice shows difficulties in their understanding and application, so that uniform or at least harmonized international practices would be helpful, especially in regard to cross border information flow.

(f) In no instance may space based integrated systems, for example mega satellite constellations for 5G wireless connectivity, be used to bypass existing regulations and protections for ground based systems and infrastructure. Even though users may get direct access to these space systems without ground based entry points, an effective regime for the protection of privacy, intellectual and business property and national and international security must be in place.

(g) For the same reason, space based integrated systems must not only be subject to the terms and conditions established by private operators.

Any consideration about an improvement of the legal and policy regime must take into account the forthcoming technical leap in integrated satellite applications. At the moment, law and policy makers still have time to come forward with new regulatory concepts before new technologies and integrated systems come into being.