ESPI
European Space Policy Institute

Current Legal Issues for Satellite Earth Observation

Treaty Verification and Law Enforcement through Satellite Earth Observation

Privacy Conflicts from High Resolution Imaging

Report 25
August 2010

Edited by
Matxalen Sánchez Aranzamendi
Rainer Sandau
Kai-Uwe Schrogl

Short title: ESPI Report 25
ISSN: 2076-6688
Published in August 2010
Price: €11

Editor and publisher:
European Space Policy Institute, ESPI
Schwarzenbergplatz 6 • 1030 Vienna • Austria
http://www.espi.or.at
Tel. +43 1 7181118-0; Fax -99

Design: Panthera.cc

Table of Contents

Foreword

Satellite Earth Observation applications are almost without limits. More and more policy and economic areas as well as social life rely on them as tools for achieving benefits for prosperity worldwide. Technology is progressing fast and methods for applications are continuingly extended and also drive technology development. At the same time, satellite Earth Observation has to respect existing legal frameworks. Where these do not exist, it can even create the need for establishing regulations. New satellite technologies together with broadening applications stimulate this need.

In this context, the International Society for Photogrammetry and Remote Sensing (ISPRS), the largest professional association in the field of Earth Observation applications, took the initiative through its International Policy Advisory Committee (IPAC) to bring together the leading associations in the space field to investigate specific topical questions related to the regulation of satellite Earth Observation. ISPRS teamed with the European Space Policy Institute (ESPI) and was joined by the International Academy of Astronautics (IAA) and the International Institute of Space Law (IISL) in this exercise, which led to a conference on 8/9 April 2010 at ESPI in Vienna. This international conference, with speakers from Europe, the U.S., Canada, Japan and Australia, focused on treaty verification and law enforcement through satellite Earth Observation and on privacy conflicts from high resolution imaging. Its results are contained in this publication, encompassing the elaborated presentations together with conclusions and recommendations emanating from the discussions.

This first cooperation between the four institutions was conducted in an extremely fruitful way bringing together the various communities involved in order to reach joint understandings and discussing joint approaches. It happened at a time when ISPRS is celebrating its 100th, and IAA and IISL are celebrating their 50th, anniversaries. The conference hosted by ESPI and the publication of its proceedings are intended to provide to the members of the involved institutions and all those interested in the field a reference publication for the topics discussed and a source of information as well as a manual for action for decision-makers.

Orhan Altan
President ISPRS

Rainer Sandau
Chairman ISPRS-IPAC

Kai-Uwe Schrogl
Director ESPI

Jean-Michel Contant
Secretary General IAA

Tanja Masson-Zwaan
President IISL

1. The State of the Art in Earth Observation

by Rainer Sandau

There is an increasing need for Earth Observation (EO) missions to meet the information requirements in connection with for instance global change studies or disaster detection and mitigation. This is perhaps most clearly seen in the many current moves for international co-operation in the field of environment where measurements from Earth Observation satellites are an essential element. This is especially so where we need to acquire, analyse and use data documenting the condition of the Earth's resources and environment on a long-term (permanent) basis.

For instance, in 2008 the Group on Earth Observations, which currently numbers some 74 countries, the European Commission and 51 participating organisations, has concrete plans for its Global Earth Observation System of Systems. In 2008 the European Union's Space Council continued to advance Europe's Space Policy, reaffirming the need for rapid implementation of the Global Monitoring for Environment and Security (GMES) program. On the European Commission side, GMES is currently implemented with the 7th Framework Programme on Research and Development. The contributions from the ESA member states support the majority of the GMES Space Component (GSC) programme, with Germany being the biggest contributor to the GSC programme.

Due to the immense improvements in such divers fields of technology as optics, mechanics and materials, electronics, pattern recognition, signal processing, computer technology, communications and navigation, the space borne Earth Observation is improving in all fields of resolution: spatial, spectral and temporal.

Let's first have a look on the developments in connection with spatial resolution. The first civil space-borne Earth surface imager was flown in 1972 on the ERTS (Earth Resources Technology Satellite) spacecraft, later renamed to Landsat-1. The MMS (Multispectral Scanner System) instrument provided a spatial resolution of 80 m and a swath width of 185 km. Space-borne systems reach now ground sample distances (GSD) of 0.5 meter.

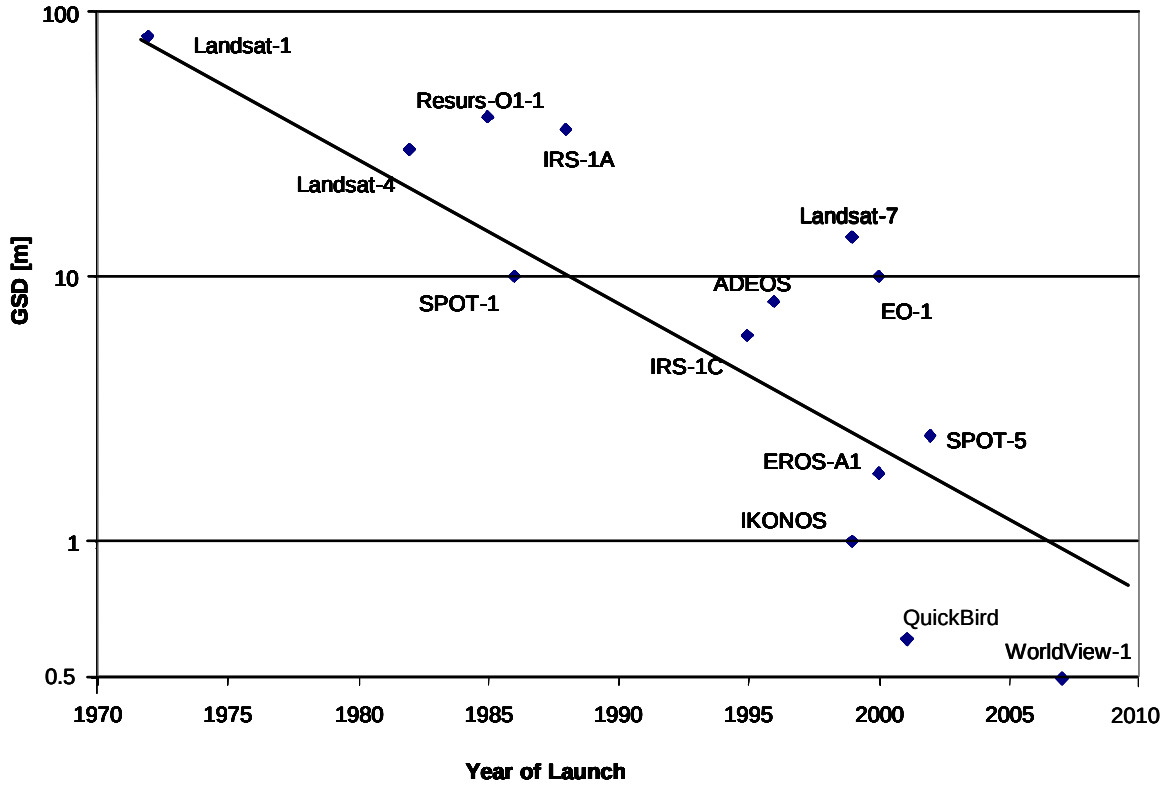


Figure 1.1: Some civil Earth surface Imagers to show the trend of ground resolution (GSD)

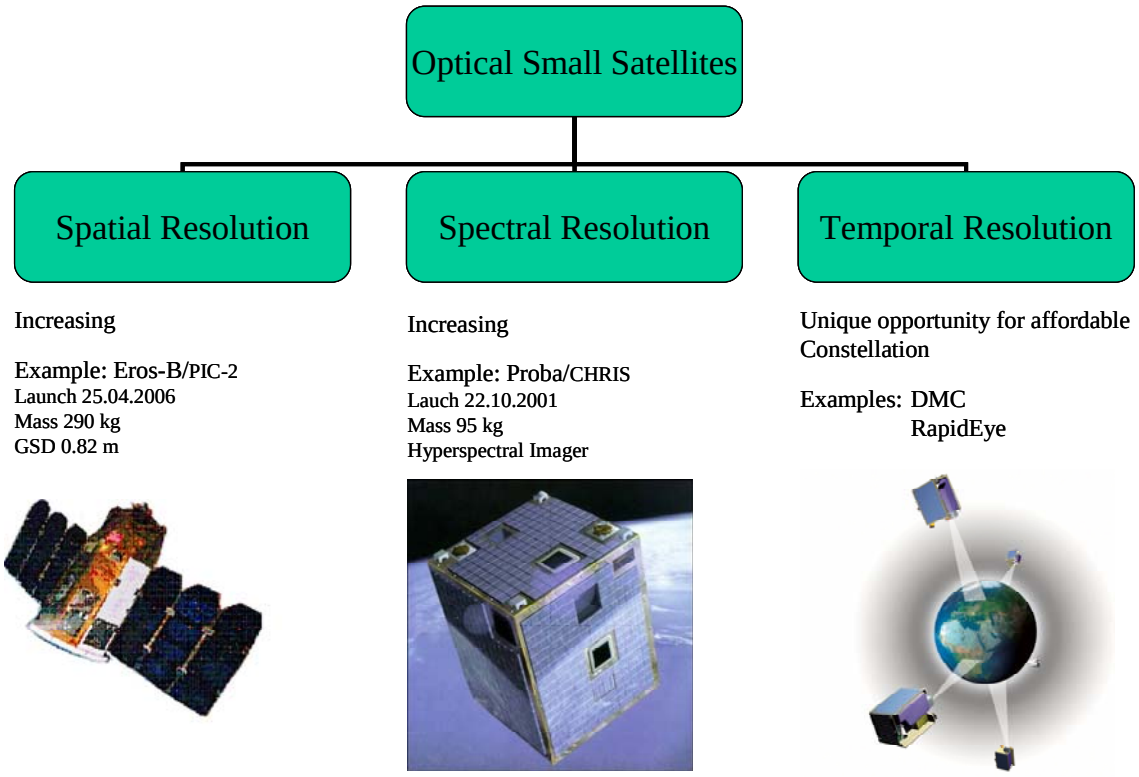


Figure 1.2: Status of spatial, spectral and temporal resolutions in the small satellite mission domain

Figure 1.1 shows the trend of spatial resolution improvement (decrease of GSD) of civil space-borne mapping systems which took place since Landsat-1 in 1972. The number of space-borne mapping systems displayed in Fig. 1.1 indicates the need of high resolution maps using the best technologies available. But besides the imaging systems shown in Fig. 1.1, there have also been developed, launched and operated many more imaging systems coming from many countries, like for instance Brazil, China, Argentina, France, India, Thailand, South Africa, Korea, UK, Germany.

The vertical axis of Fig. 1.1 is in logarithmic scale. If we first concentrate on the GSD, this value is halved in less than 5 years with respect to the horizontal axis ranging from 1972 to 2007 and the decrease from 80m of Landsat-1 to 0.5m of WorldView-1. In terms of ground pixel size in m^2, the gradient is much steeper. We observe a decrease from 80m x 80m to 0.5m x 0.5m, halving in a bit more than 2 years time in average. This is close to the numbers of Moore's law in microelectronics stating that the number of transistors on a chip is doubling every two years. Please note also, the spatial resolution progress was handicapped because of regulatory restrictions applied to civil imaging systems.

Let's now have a look on the other resolution areas. Figure 1.2 demonstrates that even small satellites are able to provide high resolution data.

Spatial Resolution

The spatial resolution is steadily increasing, i.e., the GSD is decreasing. For example: the camera PIC-2 on the small satellite EROS-B from Israel provides a GSD of 0.70 m. EROS-B with a mass of 290 kg was already launched on 25 April 2006 with a Russian START-1 launcher into 500 km sun synchronous orbit (SSO).

Spectral Resolution

Also the spectral resolution is steadily increasing. As an example may serve the hyperspectral imager CHRIS on the ESA funded PROBA satellite. CHRIS, the 14 kg/9 W hyperspectral imager, has a GSD of 18 m and provides up to 19 out of a total of 62 spectral bands in the VIS/NIR spectral range (400 – 1000 nm). PROBA with a mass below 100 kg (so it is a micro satellite) was launched into a 600 km sun synchronous orbit (SSO) on 2 October 2001 together with the DLR/Germany micro satellite BIRD for forest fire detection and fire parameter assessment, and the main payload TES (India) with the PSLV-C3 launcher from India.

Temporal Resolution

Small satellites provide the unique opportunity for affordable constellations. In this respect, small satellites can do things that are not practical to do with large satellites. At this point, DMC may serve as the example for a constellation of five small satellites. Small satellite constellations are so appealing in terms of potential temporal resolution and every day's ground coverage that even the commercial sector was triggered to launch a constellation of five satellites in August 2008, the RapidEye constellation.

The advances in the mentioned divers fields of technology support of course also the progress in EO using active sensor systems like RADAR.

We can clearly see, the already mentioned European GMES activities are based on solid ground. The GMES geo-information services will be supplied with EO data coming from a fleet of five SENTINELs implemented under the responsibility of ESA, including:

SENTINEL-1: A C-band interferometric radar mission. It provides higher spatial resolution in comparison to its forerunners ERS and ENVISAT.

SENTINEL-2: A multispectral optical imaging mission in continuation of SPOT and Landsat data provision at an improved level.

SENTINEL-3: A misson making use of an optical OLCI (Ocean Land Color Instrument), a visible/infrared radiomenter for land and sea surface temperature and a dual ban microwave altimeter.

SENTINEL-4 and 5: Two atmospheric chemistry monitoring missions, developed in cooperation with EUMETSAT, operated as payloads on EUMETSAT geostationary and polar orbiting satellites.

The SENTINELS will be complemented by additional satellites, European national and non-European, in order to fill gaps in the data supply and provide information for high resolution mapping and security tasks.

It is obvious: For EO purposes space-borne systems are important system components. The progress resulting from satellite EO allows expanding the application fields but also brings to light new problems to be discussed in a broader public debate. In this context, there are many different aspects to be investigated, two of them being: Is the existing and planned fleet of EO satellites able to support treaty monitoring and law enforcement and is it already used for these purposes? And, since the resolutions, especially in the spatial domain, are coming close to the features of ground based systems, what are the consequences in terms of privacy conflicts (individual and collective) resulting from space-borne systems.

Consequently, the conference dealt with two important and topical aspects of satellite observation:

- Treaty monitoring and law enforcement through satellite observation, and
- Privacy conflicts from high resolution imagery.

The conference brought together experts from the remote sensing and in the legal fields. It i.a aims at decision makers in the field of treaty monitoring and international law enforcement (foreign and environment ministries, international organisations). This provides the unique opportunity to discuss the different implications stemming from the technology developments and applications as well as from legal and regulatory perspectives.

The focus of the discussions at this Conference is to optimize the regulatory framework for satellite Earth observation thus supporting the full implementation of its potentials.

2. Treaty Verification and Law Enforcement Through Satellite Earth Observation

2.1 Emerging Legal Issues with Satellite Earth Observation[1]

by Ray Purdy

2.1.1 Technical Background

There have been a number of key reasons why satellite earth observation could now be more important in a legal context. Firstly, we now have many high-resolution satellites, already in orbit, with further predictions of dramatic increasing numbers, including a major growth in nano/micro/mini satellites. Any increase in the numbers of satellites in orbit, might suggest that in the future we could have access to timelier data and there will be greater coverage. This could also mean that there is increasingly better access to archived data for sale as time passes, as an increase in the numbers of images stored in archives would allow greater opportunities for looking back to see what has happened in the past. Having more operational earth observation satellites could also mean that data might be more cost-effective, as there would be more competition.

A further important advance is that, worldwide, we are seeing greater public access too and awareness of satellite Earth Observation. Google Earth is being used by members of the public not just to examine the areas that they live in, but also as a legal tool, with some even actively using it as legal evidence in planning cases. Another potential development that is also both surprising and relevant, is that it appears from my research that large numbers of people in farming communities, surveyed in the UK and Australia, actually expressed a preference to be monitored by satellite Earth Observation, rather than physical ground inspections. The majority, who liked satellite monitoring, in general terms believed it would be a more thorough and consistent method of monitoring, allowing farmers to operate on a more fair and equal basis.

However, the most important driver in terms of legal applicability is that in the last few years there has been a major step change in the spatial resolution capabilities on satellites. In the 1990s most satellites operated at resolution levels of around 30m and could only observe large land-use changes at discrete time intervals. The resolution on some satellites in 2010 is now as low as 0.50m. These dramatic resolution changes mean that in the last decade or so, high resolution satellites can now produce pictures of near photographic quality with roughly about 70 times more visibility than before. There are obviously still limits as to what we can, and can't see, and do, with current satellite data in a legal context, but what is clear is that what we can now observe from space has changed dramatically. Because of the recent advances in the technology, particularly increased availability of data at useable scales, there could now be more opportunities for the legal sector to use satellite data.

2.1.2 Monitoring and Enforcement Potential

Although these technological developments will increasingly make informed lawyers take more of an interest in satellite Earth Observation, if it is to be actually utilised in dedicated monitoring programmes under international or domestic laws, by governments, regulatory bodies or judges, then, realistically, more information as to its suitability will be required. At the very least clear, sensible advice, which does not over-sell the technology, will be required; especially as to whether satellite monitoring would work in monitoring specific types of laws, whether it offers anything different to conventional approaches, and finally, and maybe most importantly, how much it will cost. If there is no information showing one, or maybe even all of these, it is unlikely that it will be incorporated in any major monitoring strategies.

What Laws Can It Monitor?

Generally, satellite Earth Observation is very rarely used in a sustained legal context for monitoring laws, in the EU or internationally.

[1] Purdy, R "Using Earth Observation Technologies for Better Regulatory Compliance and Enforcement of Environmental Laws." Journal of Environmental Law 22:1 (2010): 59-87.
Purdy, R. "The Impact of Satellite Technologies in the International Legal Sector: The Story So Far and Implications For the Future". Derecho Espacial: Vol. XVII. Ed. Maureen Williams (Plus Ultra Press, Argentina 2010 [forthcoming]).

At the current time very few laws expressly allow for the use of satellite data in a monitoring context under legislation. Legislation in the European Union (EU) and United States (US) allows for satellite monitoring in some instances in the agricultural and fisheries sectors, but there are very few instances of it being employed in the environmental sector. One rare international example where it has been used to monitor an environmental law is its utilisation to spot illegal vegetation clearance in Australia. There have also not been many examples, worldwide, where satellite data had been used as direct evidence in a court. There again appears to only be a handful of examples of its use as evidence in courtrooms in the EU and US. Rather uniquely satellite data has been used and tested as direct evidence in courts in Australia, under the vegetation clearance legislation in each State, many more times than any other country.

Because so few legal applications for satellite Earth Observation exist in practice, with the aid of satellite technical experts, my research has examined approximately one hundred and fifty EU and international environmental laws, to consider possibilities for new applications. This research found that many environmental laws could actually be monitored to some degree by satellite earth observation. Environmental laws in sectors including waste, water, dangerous substances, air pollution and climate change, and land and nature protection could in some circumstances be monitored this way. However, its potential as a monitoring tool should not be overstated. Satellites could not monitor every environmental law as they can not see inside buildings. For some other laws, such as those governing air pollution they can be unsuitable because they are not always capable of the temporal sampling and averaging necessary to determine exposure over short timescales, or satellite-based sensors can not always measure some constituents of a polluted atmosphere. Some further forms of monitoring were achievable but were incompatible with the law itself; e.g. air pollution monitoring has to be monitored at ground level in some EU legislation. However, this does not mean of course that current laws cannot be changed, or future laws developed with the use of satellite data in mind.

To test the value of satellite Earth Observation as a tool for legal monitoring, archived imagery was also obtained during the course of my research, which corresponded to actual prosecutions that had already taken place, providing the basis for original analysis of where satellite data could be used to detect breaches of environmental laws. This found that, generally, there is a broad range of opportunities that the imagery offered and three specific uses in particular could be highlighted. The first of these is that they can be utilised by regulators as part of a targeted enforcement strategy. A core example in using satellite Earth Observation data in this way is again from Australia, where it has been used in an attempt to curb illegal deforestation and vegetation clearance associated with farming and development activities.

A second area where satellite Earth Observation might have a strong value to lawyers is monitoring individual sites or areas where environmental offences have been known to occur historically. To demonstrate this, my research identified a UK court case, where a defendant was convicted of storing large numbers of scrap vehicles on a site without a waste management licence and was ordered to remove them by a court order. Satellite imagery obtained several months after the court decision, showed that the defendant had not complied with the timing of the court order to remove the illegal vehicles from this site.

A third potential area of legal interest for satellite Earth Observation is its use as a form of historical evidence. Systematic archiving of satellite images could in theory provide regulators or a court with a relatively impartial snapshot of any location at any given time, providing accurate evidence that would be otherwise unavailable. To test this, my research identified a UK court case where a defendant was convicted of running an illegal waste disposal operation. The defendant in this case was financially profiting from the burning of hazardous wastes on his land between May 2005 and January 2006. Satellite images which I obtained during this period clearly showed the burnt area of land where this took place. Satellite images which were taken a year before the regulator believed the offence was committed appeared to show a large burned area on the land in June 2004 and might have been used as evidence that the illegal activity has been ongoing for a longer period of time than the investigators thought. This highlights the practical function of historical archives of satellite images for prosecuting authorities.

Although there are extensive archives and catalogues of satellite images, like the ones I used in my research above, it is still not possible to have access to all historical satellite data. Whilst satellites are constantly collecting data, this information is not always kept long-term, primarily because of the massive computer data storage space requirements. Because of storage difficulties, some archives only contain data that distributors think peo-

ple will buy, so there is far greater chance of finding archived images of cities and industrial areas than rural ones. If information about an activity that had taken place in the past, on a particular day was required, in most cases it would be unlikely that imagery would be available. So monitoring polluting activities where the temporal dimension is tight, such as oil pollution discharges from tankers at sea, could therefore be difficult using orbiting satellites. If one only required a snapshot of an activity taking place over a longer period of time, like the waste burning example above, it would be easier to find relevant imagery.

Advantages over Conventional Approaches?

Satellites appear to have some advantages over other similar forms of monitoring, such as aerial photography, by having greater coverage – both in terms of area and revisits. Whether this form of monitoring is more resource efficient in practice obviously depends on the actual law being monitored, but in some instances there is a strong case that it would be. Each year in Europe, over 5 million farming businesses declare more than 50 million agricultural parcels when claiming EU subsidies. That is a lot of farms to check in every EU Member State country. With satellites, regulators can do this much more quickly and easily than by sending in inspectors on the ground. Similarly, in Australia there is no way that inspectors could monitor vegetation clearing laws by ground-based monitoring alone, as some of the distances between cities and farms are enormous. It might take an inspector a whole day just to drive to the farm under investigation, and many more hours or days to map the land. Satellite imagery can obviously give regulators a 'first-look', before deciding whether to send an inspector to the farm itself. This method can enable them to look at a lot more farms than ground monitoring alone, and target those inspections that they do undertake more effectively.

Satellite Earth Observation is different to other forms of surveillance because those being monitored in this way can be informed that they might be monitored, but they can't tell when or whether they are being watched. This appears to have had a strong influence on the compliance behaviour of those subject to regulation. Research that I have undertaken, surveying United Kingdom and Australian farmers, found that the majority of those questioned did not know how regularly they were monitored by satellites. UK farmers greatly overestimated both the percentages of farmers monitored this way annually, and the number of checks made by the satellite. Conversely, farmers in Australia actually under-estimated the true extent of how often they were monitoring. Significantly, however, over half of all the UK and Australian farmers surveyed agreed that satellite monitoring was acting as an increased deterrent. The potential of Earth Observation satellite monitoring to act as a smart deterrent method might progressively catch the attention of regulators seeking new enforcement strategies.

More Cost Effective

Regulatory bodies increasingly have to cope with funding constraints that require them to reconsider their conventional ways of monitoring and enforcing laws. The volume of laws has increased but the numbers of staff charged with monitoring and enforcement has in many countries remained static or often decreased. This is even truer at the moment, when parts of the world are struggling with economic recession. Such bodies are, therefore, in the difficult position of finding the regulatory 'holy grail' of effective monitoring with ever more constrained resources.

When compared with some forms of ground-based monitoring, it is conceivable that in certain circumstances, monitoring using satellite Earth Observation could offer financial savings. There is little hard data available as to the cost effectiveness of satellite monitoring over field inspection based monitoring. However, the purchase of satellite data from commercial providers to check the minimum levels of claims in all European Member States, for agricultural subsidy payments, costs the EU approximately 5 million Euros each year. For subsidy monitoring this appears to be a more cost-effective method of monitoring because it has resulted in significant financial savings at national level compared to the cost of ground inspections, and the EU stands to save money if the subsidy fraud levels go down, which they also appear to have done.

2.1.3 Privacy Issues with the Use of Earth Observation

Whatever the potential of Earth Observation data as legal evidence, it is clear that its use in court raises a number of important issues in respect to its admissibility under existing evidential rules. Obviously different countries and even types of court will be subject to different evidential rules, but generally it seems quite unlikely that rules of admissibility will prohibit the use of satellite data *per se*. However, many countries have national legislation that protects privacy and it is pos-

sible that some courts could exercise their discretion to exclude evidence on the basis of privacy rights.

It is a moot point whether the current resolution of satellite imagery is sufficiently intrusive to interfere with a person's private life, as protected under some countries legal systems. However, what seems to mark satellite Earth Observation out from other similar forms of surveillance is the fact that it is covert; it can be more intensive and extensive; and it can potentially monitor everyone - as it does not distinguish between public and private property. Surveillance which has the capacity to be intrusive is usually controlled by Government, but satellites are not currently subject to any controls and we have the unusual position where often fully commercial companies are controlling a potentially invasive technology.

In Europe it is normally for the person complaining to prove how an activity has affected his rights; the court then considers whether it was an interference or not and then the aim of the activity. It is unlikely that much of the current satellite data which is commercially or freely available could be successfully argued to be intrusive, particularly if what could be seen on the image could be seen from, for example, any public road. The question of how much privacy people are entitled to in relation to satellite monitoring, however, remains untested in the courts. But as the resolution improves and the frequency of the data being used in the courts increases, it is only a matter of time before a well informed lawyer will seek to raise this as an argument for the defence.

Connected to privacy rights in a legal context, is also public acceptability. There are wider, more fundamental questions about monitoring people in this way. Those wishing to use satellites in a legal context might also need to secure public acceptance of and confidence in the technology. Even applications like Google Earth might be less acceptable to some people or groups if more advanced resolution imagery is placed free online. There has been very little effort to try and conceptualise how a regulated community feels about satellite surveillance. Surveys I have undertaken in both the United Kingdom and Australia appear to show that the majority of those monitored this way by regulators consider it to be an invasion of privacy. In both countries over half of the farmers felt that this method of monitoring was invasive. Respondents who were against satellite monitoring indicated their dislike at being watched in a covert 'big brother' fashion. Many specifically related satellite monitoring to George Orwell's novel *1984*. Some also perceived that they were treated at guilty until proven innocent.

Issues of privacy may prove more problematic as the technology develops. It is unclear where we are heading with resolution levels on satellites and whether we have reached a plateau, or if the technology will continue to develop to as low as a few centimetres in the future. Whilst this could enable great monitoring opportunities, suitable safeguards will have to be developed to balance the competing interests involved. There needs to be greater consideration of and public debate over what we find to be acceptable or intrusive monitoring, now, rather than as a knee-jerk reaction later to future step changes.

In the surveys I undertook, attitudes towards satellite monitoring, in the context of privacy, softened if those monitored this way were told of the monitoring, if they could have access to the data, if they were given assurances with regard to data information security, and if there was adequate protection in the courts in case there was abuse of this data. However, different perspectives on privacy rights could mean that what might be acceptable in one country might not be in another. At the very least governments wishing to use satellite monitoring might have to justify to their citizens why it should be used and to also undertake some form of privacy impact assessment, to make sure it does not have any detrimental impact to privacy – either of the targeted group or from collateral viewing. Such things exist for CCTV, and whilst its international impact makes this form of regulation more complex, there is still potential for similar schemes to operate in relation to satellite monitoring too in relation to legal enforcement.

2.1.4 Future Initiatives in Satellite Earth Observation

If satellite Earth Observation is to be used more in legal strategies in the future, then the technology itself needs a significant user push. Companies that design, launch and sell the data should be targeting the legal community as a potentially significant market for satellite data. Clearly, Earth Observation data could be a valuable source of evidence to regulatory bodies and police, as well as the estimated eleven million lawyers practising world-wide. To successfully reach these groups, and implement Earth Observation into legal strategies, there will be a need for strong advocates and effective champions for these technologies who can persuade others of the utility of Earth Observation. Under GEOSS and GMES, foundations have been built for future progress, but it is unclear

whether these initiatives could themselves oversee or take direct responsibility for the coordination of legal opportunities and the implementation of high-profile pilot demonstration studies. There is now a need for a body to show dynamic leadership and play a coordination role, identifying strategies for enhanced profile building to legal audiences.

Closely connected to the above point, is that there is currently little interaction between lawyers and technical specialists in the satellite Earth Observation field. In practice the development of Earth Observation has been almost exclusively technology-led to date and a major long term obstacle to having more legal applications in this area is this lack of communication between disciplines. The mainstream development of Earth Observation in the legal sector might not be stimulated until greater joined-up thinking and cross-disciplinary cooperation occurs; allowing for future technologies to meet legal users' needs by being bespoke commissioned for specific purposes and applications. The groups charged with leadership should consider new innovative approaches to overcoming this barrier, and introduce imaginative and attractive new methods for fostering interdisciplinary cooperation.

Although Google Earth has had an impact in raising awareness of Earth Observation, it is highly likely that most of the legal sector would have never seen a satellite image in a legal context. For example, I came across a judge in Europe who, when presented with a satellite image, queried how long a man needed to spend in the satellite taking pictures. Clearly, very little effort has been made to educate the legal sector to date, with very few bodies taking institutional or leadership responsibility for raising awareness of the advantages and limitations of using satellite data. It would be a frustration if the profile raising and cooperation discussed above were to succeed, only for problems of understanding or acceptance within the courtroom to occur. There is therefore a pressing need for knowledge transfer, capacity building and training in the legal sector, from early career lawyers to senior judges.

Connected to judicial understanding, is the issue that there are currently no international rules or standards in place as to the use of Earth Observation as evidence in the courtroom, which, were they to exist, might give lawyers greater confidence in the use of the technology. Again it would seem impractical to champion the technology only for it to encounter problems with its actual weight as evidence. There are many comparative examples, such as rules governing digital CCTV images or speed cameras that can be applicable as templates in designing such rules or standards as to its use as evidence. We are also seeing specific Earth Observation focussed national schemes being developed in a couple of countries across the world, in direct response to this issue. Although there is a creep of developments at national level it seems that there should be the introduction of an international best practice scheme and someone should take ownership of this. There are arguments both for and against this being overseen under the banner of GEO or GMES, a body like International Standards Organisation, or another legal group, but someone needs to take responsibility for this issue in the next few years.

2.2 What's in GMES for Treaty Monitoring and Law Enforcement[2]

by Gunter Schreier

2.2.1 The European GMES Scenario

The EU Member States have strengthened their common policies in the treaty of Lisbon, which entered into force on 1 December 2009. The treaty sets the common understanding of the EU Member States to work together on issues of environmental protection and civil security on a legal binding basis. Article 189 of this treaty also calls for a European Space Policy and to take the "necessary measures" to implement it.

[2] Treaty of Lisbon, English Edition, Official Journal of the European Union, C306, Vol 50. 17. Dec 2007
TanDEM-X, Die Erde in drei Dimensionen, DLR Folder; Cologne, November 2009.
Zink, M.; Fiedler, H.; Hajnsek, I.; Krieger, G.; Moreira, A.; Werner, M. "The TanDEM-X Mission Concept." IEEE Geoscience and Remote Sensing Symposium, 2006. IGARSS., July 31- Aug 4, 2006.
Duformont, H. "The INSPIRE (2007/2/EC) data policy." GENESI-DR workshop presentation Ispra, Italy, 26. January 2009
02 July 2010 <www.genesi-dr.eu>.
Implementation Guidelines for the GEOSS Data Sharing Principles; Document 7(Rev2) GEO-VI; 17-18 November 2009
Joint Principles for a GMES Sentinel Data Policy, ESA/PB-EO(2009)98, rev. 1 Paris, 23 October 2009
Hernandez, M. "UNESCO and partners, an Open initiative on the use of space technologies for the conservation of natural and cultural heritage." Use of Space Technologies for the Conservation of Natural and Cultural Heritage, Campeche, 28 November – 2 December, Mexico.
Satellite Data Security Act; Federal Gazette (BGBI.) year 2007 Part I No. 58, Issued in Bonn on November 28, 2007.; Unofficial English translation in Journal of Space Law 34 1 (2008)
GeoHR "Hand-outs of HR Geo user consultation workshop" ESA ESRIN, Frascati, Italy, April 16th, 2010.

Figure 2.1: GMES Services Core projects and Primes of pan-European Teams

Apart from European autonomy in satellite based navigation (i.e. the Galileo Program), EU Member States recognized the suitability of space technology – including Earth Observation from orbiting satellites - to help to preserve the environment, to protect the climate and to safeguard the security of its inhabitants.

European plans and capabilities to meet this challenge are being brought together in the GMES program (Global Monitoring for Environment and Security). Its purpose is to establish satellite systems and related ground infrastructure in Europe for Earth Observation and to provide geo-information services for citizens of Europe and of other countries.

The GMES program was first initiated in a European conference in Baveno, Italy, in 1998. Since then it got momentum and was officially agreed to be implemented as a joint activity under the leadership of the European Commission, wherein ESA (supplemented by contributions from EUMETSAT) is taking care of the management of the space segment and the Commission is responsible – apart from the overall management – for the development and the sustainability of the geo-information services. On the Commission side, GMES – and specifically the five selected geo-information services (Figure 2.1) – is currently implemented with the 7th Framework Programme on Research and Development, whereas ESA member states contributions support the majority of the GMES Space Component (GSC) programme.

The successful implementation of this ESA programme was highlighted at the ESA Ministerial in The Hague in November 25–26, 2008, with Germany being the biggest contributor to the GSC programme.

The GMES geo-information services will be supplied with Earth Observation data from a GMES fleet of satellites. The first component of this fleet will consist of five series of GMES SENTINELs, implemented under the ESA GSC programme:

Sentinel-1: a C-band interferometric radar mission, providing continuity to the ERS and ENVISAT Satellites, but with higher ground resolution and more capacity per orbit.

Sentinel-2: a multispectral optical imaging mission, providing improved continuity for SPOT and Landsat kind of multispectral optical data.

Sentinel-3: a mission with a dual band (Ku and C) microwave altimeter, a wide-swath optical imager (OLCI = Ocean Land Color Instrument) with 21 channels and a visible/infrared radiometer for sea/land surface temperature observation.

Sentinel-4, -5: two families of atmospheric chemistry monitoring missions, developed in close cooperation with EUMETSAT and operated as a dedicated payload on EUMETSAT geostationary (Sentinel-4) and polar orbiting (Sentinel-5) satellites.

These SENTINELS will be complemented by additional European national and non-

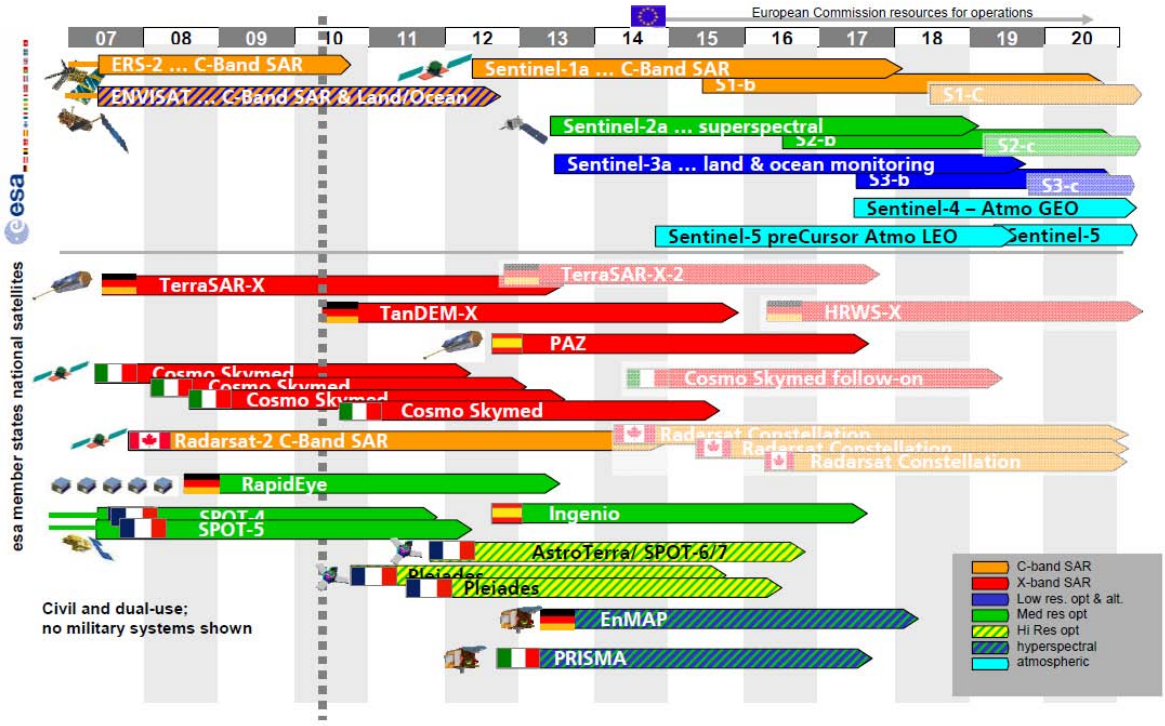


Figure 2.2: GMES SENTINEL and European contributing Missions

European (3rd party) satellites to fill gaps in the data supply and to deliver information for high resolution mapping and security-relevant tasks (Figure 2.2).

Baseline for the access to the orbiting satellites will be multi-mission ground segment, based on national facilities, data centres and near-polar acquisition stations. These stations are complemented by (at least two) geostationary European Data Relay Satellites (EDRS), allowing real time programming and data transfer to those SENTINELS (currently 1 & 2) and national missions (currently TerraSAR-X and post-TerraSAR-X missions) equipped with appropriate Laser Communication Terminals (LCT).

2.2.2 German Space Segment Contributions to GMES

Apart from its financial contribution to ESA and EU GMES programs, Germany contributes several Earth Observation systems – already in space or to be launched – to the GMES programme.

TerraSAR-X: launched in June 2007, this very high resolution multi-mode X-Band SAR satellite is operated as a Public Private Partnership (PPP) between DLR and the company ASTRIUM/InfoTerra. Its phased array X-Band SAR antenna and the precision of the geolocation of SAR pixels are already now subject to innovative applications such as moving object detection and repeat pass SAR interferometry.

TanDEM-X: launched on June 21st, 2010, TanDEM-X is the twin brother of TerraSAR-X. Manoeuvred in a unique helical orbit with TerraSAR-X, this TanDEM-X satellite will circle around TerraSAR-X just a few hundred meters away and will form the first bi-static SAR interferometer in space in order to generate the most precise global Digital Elevation Model (DEM). (DLR, 2009; Zink 2006).

RapidEye: The constellation of 5 small satellites was successfully launched in August 2008 from Baikonur. Each of the five satellites carries a 5 band push broom scanner at 6,5 m GSD. The constellation enables a daily coverage of all land masses of the earth. RapidEye is owned and operated by RapidEye AG of Brandenburg, Germany (www.rapideye.de).

EnMAP: A DLR owned and operated hyperspectral imaging mission with >200 spectral channels at 30m ground resolution and 30km swath. EnMAP is scheduled to be launched around 2013 and will primarily serve science needs, whilst operational applications should be demonstrated.

ResourceSat and CartoSat: The company EuroMap; Neustrelitz, Germany, holds the exclusive European acquisition and marketing rights for the Indian Remote Sensing (IRS) satellites (www.euromap.de). The IRS-P6 (ResourceSat) is the current working horse

for European land coverage. The IRS-P5 (CartoSat-1) with its 2.5 m in track stereo b/w capability is a unique source of Digital Elevation Model (DEM) information. EuroMap and DLR are teaming to downlink and process the data at the DLR facility in Neustrelitz.

IKONOS and WorldView-1/2: After having access to the IKONOS satellite, the company European Space Imaging (EUSI), Munich is now teaming with DigitalGlobe to have direct access to the WorldView-1 and -2 satellites (www.euspaceimaging.com). The latter has 0.5 m resolution and is tasked from and acquired by a station at DLR, Oberpfaffenhofen. All these very agile and responsive submetric satellites form the basis for many GMES applications such as emergency mapping and civil security.

2.2.3 Treaty Monitoring & Law Enforcement in GMES. Past and Ongoing Projects

As mentioned above, the demand of GMES for geoinformation services and hence the need for satellite data, is governed by core application projects. These projects are implemented in the framework of FP7 as large pan-European pre-operational implementation tasks, directing the way for an initial full GMES operations from 2014 onwards. These core projects had precursors and accompanying other projects of similar topics both in the European Commission framework research programmes as well as in ESA projects. For the specific case of civil security (and focussing on those with DLR involvement), these GMES projects are briefly depicted below.

2.2.3.1 Global Monitoring for Security and Stability (GMOSS)

GMOSS was implemented as a late FP6 call and lasted from March 2004 to February 2008. The 22 partners were coordinated by DLR. GMOSS was an action, where the EC contributed to the exchange between scientists and users and paid for workshops and meetings. Hence, rather than new developments, existing expertise in using Earth Observation data for civil security in Europe has been gathered and perspectives for future applications have been given.

Specifically, an analysis of the potential of remote sensing for the following applications was performed:

- Monitoring of international treaties protecting against the proliferation of weapons of mass destruction
- Monitoring of critical infrastructure
- Monitoring of borders
- Threat analysis and early warning

The analysis was accompanied by practical test cases and intensive dialog with the users of the derived information, such as the International Atomic Energy Agency (IAEA) in Vienna. An example for monitoring international treaties is given below. Earth Observation data has been used since the very beginning of this technology to monitor critical developments with regard to the proliferation

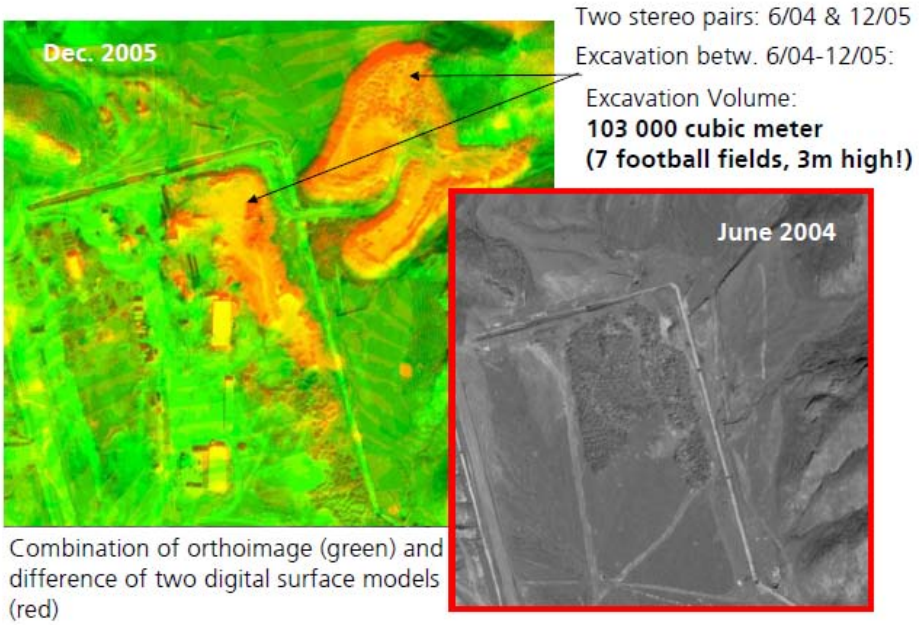


Figure 2.3: Subsurface construction monitoring using QuickBird satellite data at the Esfahan, Iran, nuclear facility, Analysis performed by DLR in GMOSS project

of weapons of mass destruction. Whilst during the cold war classified military reconnaissance primarily targeted the areas of influence of the nuclear super-powers, nowadays areas of interest are emerging nuclear powers. As far as seen from space, such developments can now be monitored by using unclassified commercial satellite data (figure 2.3).

GMOSS laid the way for the implementation of "Civil Security" as one GMES core service. GMOSS has clarified the capacity of European technology and know how in this domain, identified the needs for European and international organisations and discussed issues such as the politically sensitive cases and the confidential treatment of some of the information derived.

2.2.3.2 Land and Sea Integrated Monitoring for European Security (LIMES)

LIMES was also implemented as a late FP6 project and lasted from December 2006 until May 2010. 46 European partners were coordinated by e-GEOS, Italy (the former Earth Observation branch of Telespazio). LIMES continued with the topics of GMOSS, but added research and development in image analysis and GIS technologies. Applications focussed on:

- Treaty Monitoring, land & critical infrastructure monitoring
- Surveillance of EU borders (land and sea)
- Supporting non-proliferation treaty monitoring

Focus was given on applications in the European area and a close liaison with European national users. For example, in the framework of LIMES, DLR initiated an R&D partnership with the German Federal Police (BKA).

A series of international workshops highlighted European capacities but also clarified the limitations of Earth Observation technologies in civil security applications. Though some of the users were at first disappointed to notice that an omnipresent observation from space with life images in the range of cm resolution (as seen in some Hollywood movies) is not possible, most of them recognized the unique capabilities of Earth Observation in some domains of civil security and law enforcement.

LIMES was then continued by the implementation project of the theme "civil security" in GMES: G-MOSAIC.

2.2.3.3 GMES Services for Management of Operations, Situation Awareness and Intelligence for regional Crises (G-MOSAIC)

G-MOSAIC – the implementation of a pre-operational GMES core service - primarily aims at EU security related to „out of EU area crises", for *inter alia* peacekeeping and peace-building. G-MOSAIC has 36 partners and started in January 2009 with an expected duration of 36 months. It focuses on three main themes:

- Monitoring of treaties for non proliferation
- Monitoring of illegal activities
- Monitoring of routes and borders

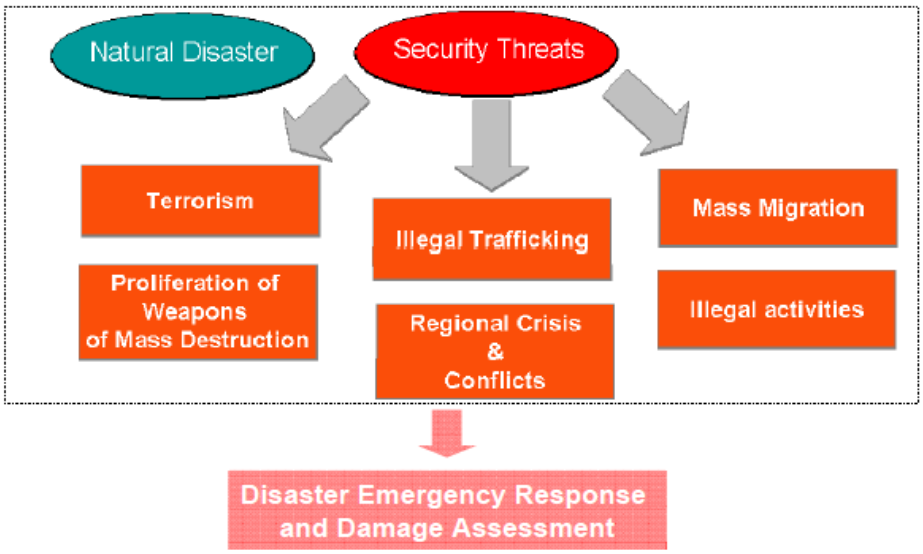


Figure 2.4: Areas of interest and services of the G-MOSAIC GMES project

The security aspects of GMES are carefully addressed not to interfere with military interests or domain. A clear need for comprehensive non-military situational awareness was stated in the projects so far. However, complex international situations may not be able to distinguish both domains. Military forces of European countries are now involved with military and civil personnel in regional crisis situations around the globe. The European Common Foreign and Security Policy (CFSP) and the Lisbon Treaty defined a clear role and responsibility of the European players in this domain.

2.2.3.4 European Maritime Security Services (MARISS)

Synthetic Aperture Radar (SAR) technology has the unique capability to actively work day and night and to penetrate clouds. Metallic objects on an otherwise flat environment can easily be distinguished in space borne SAR images, even if the resolution of the SAR may be not sufficient to identify details of the object. Hence, ships on water bodies can be identified at every time of the day. A broad image "swath" (i.e. size of the image) and frequent revisit of the orbiting spacecraft

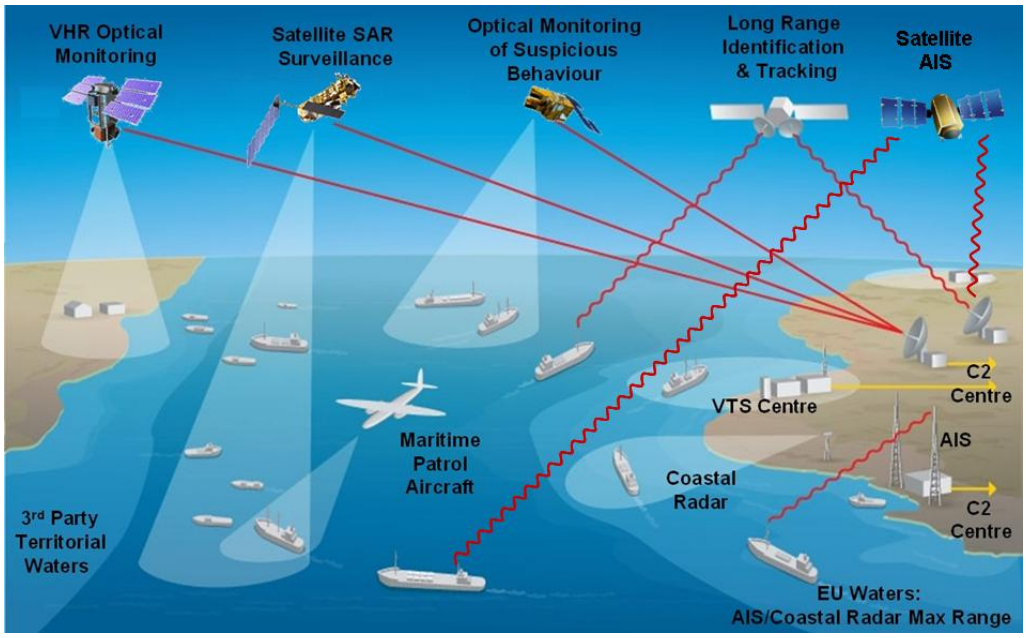


Figure 2.5: Space based technologies for maritime security (as used in the MARISS project)

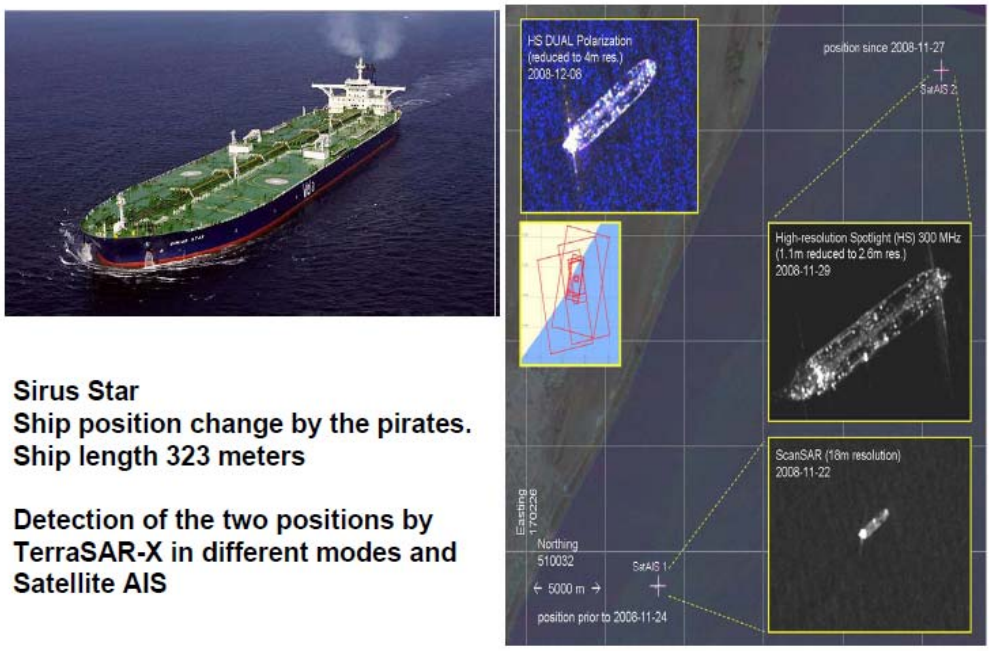


Figure 2.6: Detecting the high jacked Sirius Star by TerraSAR-X SAR near the coast of Somalia. Analysis performed by DLR

would allow monitoring all European coastal waters. On top, ships larger than 300 tons need to identify themselves with an electronic identification signal (AIS: Automated Identification System), carrying the name, location and further information. Meant to work only in coastal areas, AIS signals can now be picked up by space based receivers. The verification of both technologies – SAR based ship detection and space based AIS reception – is performed in the ESA GMES project MARISS (European Maritime Security Services) (figure 2.5). MARISS is now extended to a "Scaling-Up" Phase (MARISS-SUP) lasting to about 2012. Eight partners set-up a coordinated Service Network to provide maritime European user organisations with integrated ship detection services. Key for ship detection is the fast access to and the fast processing of the data. Therefore, most MARISS partners own and operate a radar satellite receiving station (figure 2.7). DLR contributes to MARISS-SUP with its station in Neustrelitz, Germany (acquiring ERS-2, ENVISAT and TerraSAR-X data) and a station, which DLR is operating in cooperation with Mexican authorities in Chetumal, Mexico (acquiring ERS-2 and TerraSAR-X).

The maritime security application of MARISS is a special case for GMES, insofar dedicated European organisations have expressed a clear need and already use SAR data for maritime applications; namely the European Maritime Safety Agency (EMSA) in Lisbon, Portugal. EMSA was created in 2002 after a series of disastrous tanker accidents with subsequent oil spills, spoiling European coasts. In its CleanSeaNet programme, EMSA is already using satellite SAR to monitor European coastal waters. The CleanSeaNet2 programme, starting end of 2010, now also adds the demand to detect ships and to use AIS information for ship identification. EMSAs motivation here is to possibly also identify the source of oil slicks found in SAR images. But EMSA (in cooperation with FRONTEX and national maritime organisations) also investigates SAR ship identification capabilities to support the international forces in securing the East African waterways against piracy (figure 2.6).

SAR and AIS based ship detection for security applications is part of the core GMES project G-MOSAIC. However, operational use of this application is already implemented by EMSA and other organisations. These organisations adapt to the mechanisms ESA and data suppliers have implemented for Earth Observation data access.

Figure 2.7: Areas of interest and services of the G-MOSAIC GMES project

2.2.4 Data Policies for German National Missions

Germany has launched two very high resolution SAR missions in Public Private Partnership (PPP). After the launch and operations of TerraSAR-X in 2007, the twin brother of TerraSAR-X, TanDEM-X was successfully launched on June 21st, 2010.

The availability and distribution of submetric, high quality SAR data over global terrain required a clear regulation on how the national security interests of Germany and its partners are not affected by SAR based intelligence availability over critical areas. Considering the international regulations and the objective to develop the commercialisation with clear supporting guidelines rather than a restrictive case-by-case basis process, and taking a general approach beyond SAR observation technology, Germany developed the Satellite Data Security Act (SatDSiG) which entered into force December 1st, 2007 (German Federal Gazette, 2007).

The Act addresses only German satellites, operated by German citizens. Hence the acquisition and distribution of Indian and US satellite data by German companies/ entities is not affected and assumed to be regulated under corresponding Indian and US law. Further on, the Act does not concern governmental satellite systems, which work for military/intelligence services.

The regulations of the Act only apply to "high grade" Earth Observation systems. The definition of "high grade" is described in the Act and consists of defined limits of geometric and spectral resolution, amongst others. Whereas, TerraSAR-X is regulated under the Act, the optical resolution of RapidEye and EnMAP is regarded as uncritical under the Act.

The Act requires an operator license for the operation of a high-grade Earth remote sensing system (Part 2, Section 3) and a dissemination license for the dissemination of data of such a high-grade system (Part 3, Chapter 1, Section 11). In practice the Act is clearly focussed on a clear and transparent procedure for the first time dissemination (both science and commercial) of Earth Observation data. “First time” here means that all data use/dissemination beyond the initial data distributors, directly responsible to German law under the Act, shall not be directly affected. For TerraSAR-X, two German entities have got appropriate governmental licences: DLR for the mission operations and distribution of data to science users and Infoterra for the data distribution under the commercial scheme.

This license is only granted to entities, which demonstrate a significant degree of liability and have technical means to protect the access to the data. The latter includes that all commands to the satellite are generated in Germany and are encrypted by an admitted encryption scheme. A secure encryption mechanism applies also to the down linked data, as well as further secured archiving and distribution mechanisms. Commercial partners need also to show protection for foreign business takeovers.

The distribution of the data outside this secure perimeter to national and international users is governed by a “sensitivity check” in a decision tree (figure 2.8). Therein, the category of users, a positive and negative list of target areas, the geometric resolution and the timeliness from data sensing to product delivers (i.e. near real time applications), determine whether a product can directly be delivered to international users or the delivery needs a permission by the governmental authority in charge (here: Federal Office of Economics and Export Control, BAFA). The sensitivity check is under the full responsibility of the licensee. Demands from “critical customers” can be evaluated by BAFA in advance to allow transparent business cases.

2.2.5 Some Technical Considerations on EO Data for Treaty Monitoring and Law Enforcement – Global Presence

Many applications in treaty monitoring do not demand very fast access to Earth Observation data (e.g. the monitoring of nuclear facilities), but the creation of long or seasonal time series to monitor change, which might indicate the violation of treaties. However, especially law enforcement demands very fast presence and very fast access to the data taken over the event or area in question.

Detecting oil spills and in the same image, detecting the ship which might have caused the spill, asks for only about 15 minutes between the image data take and the detection of the spill. When significant more time has passed, there is often no change to catch the violator in action. This “near real time” (NRT) demand is shared by most law enforcement actions and the use of Earth Observation data monitoring the extent of disasters. For the latter it is critical that external support and humanitarian aid is brought to the place of destruction as fast as possible.

Nowadays polar orbiting Earth Observation systems can often not meet these NRT requirements. Firstly, the orbiting satellites only scan a certain area every other day or so (means: a continuous or several-time-per-day monitoring is hardly possible). Second, remote areas can be monitored, but the data need to be recorded on board and can - only after minutes or hours – be down linked to the next operating ground stations.

Therefore, GMES has included in its space assets European Data Relay Satellites (EDRS), which reside as communication towers in geostationary orbit positions and can communicate with appropriately equipped Earth Observation satellites at virtually any position on the globe. Starting by 2012, ESA plans to deploy at least three of these communication satellites. The fastest communication link will be a Laser Communication Terminal (LCT) with up to 5.6 Gbit/sec transfer rate. In parallel, at least Sentinel 1a and Sentinel 2a will be equipped with an LCT. It is planned to also mount such communication means to the TerraSAR-X follow-on satellites.

Geostationary relay satellites and communication terminals would allow global and instantaneous access to the imaging satellites, but would not solve the problem of the time it takes for an imaging satellite to pass over a region of interest. Two principal solutions are currently under investigation (and partly under implementation) to address this challenge.

Constellations of Earth imaging satellites just put more satellites in orbit to lower the time it takes to revisit a certain area. Existing examples are the Cosmo-Skymed satellites (4 SAR satellites in full deployment) or the RapidEye constellation (5 optical satellites, allowing daily revisit in 6.5 m resolution). The use of many satellites of the same kind but from many nations and operators, is a strategic approach in GMES to reach for global and frequent coverage of hot spots on Earth.

A more visionary proposal in this domain was made by the satellite communication company IRIDIUM, which offered to deploy Earth Observation payload on each of its 66 NEXT generation LEO communication satellites. Whilst high resolution imagers seem not possible under current technical and financial limitations, proposals are under investigation to put some Earth science payload at least on some of the NEXT satellites.

Another technical solution for global and immediate presence is to use the geostationary orbit to have visibility of an entire Earth sphere. This approach is used already in geostationary weather satellites (with several of these in operations). Though, imagers on geostationary weather satellites capture the entire globe with up to 15 minutes revisit/re-imaging time, their geometric resolution is technically limited (both by e.g. optics and data rates) to about one kilometer per pixel. Not enough to use the data for treaty monitoring and law enforcement applications. Therefore, new concepts have been studied to increase the resolution of geostationary imagers, mapping only parts of the globe and

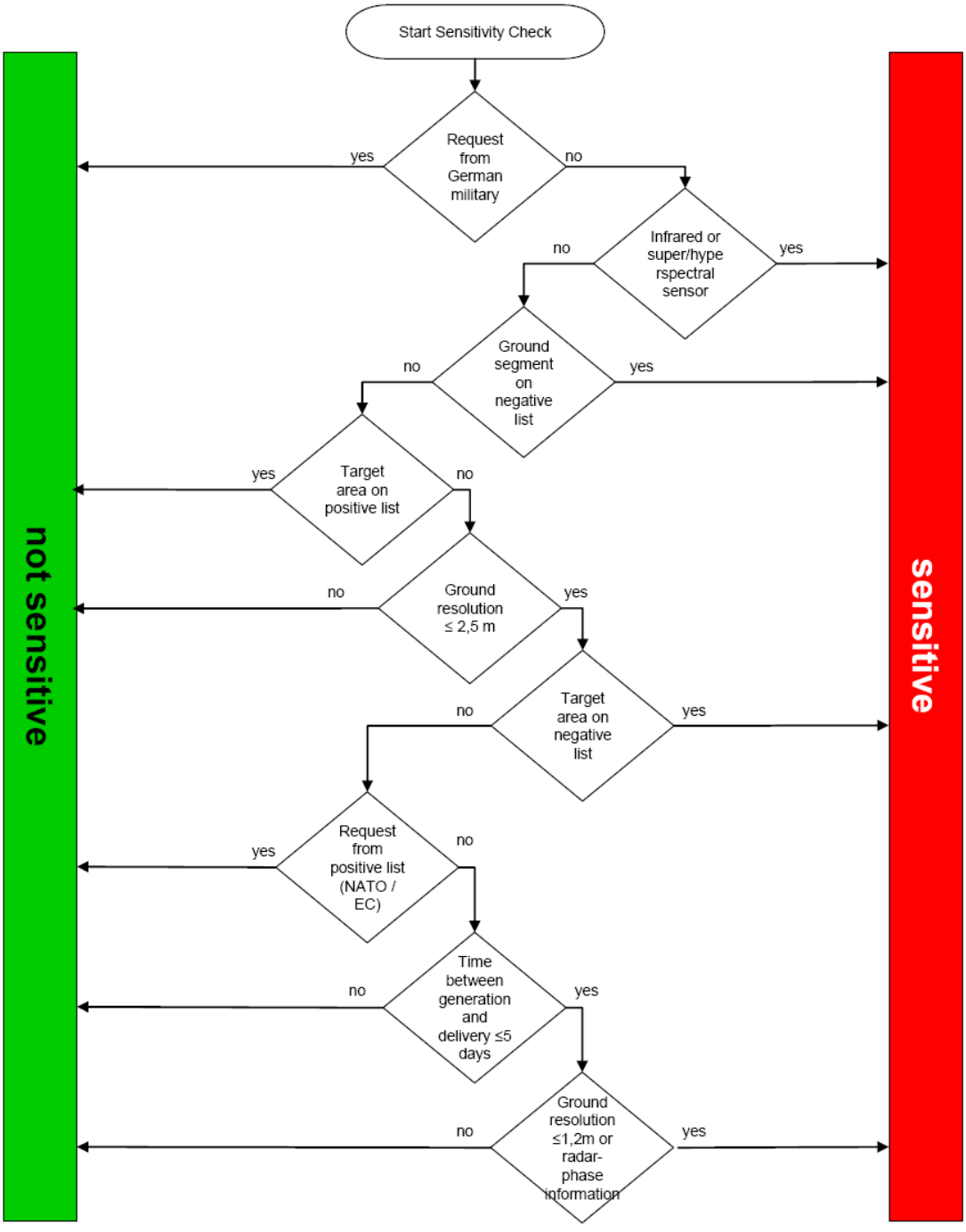


Figure 2.8: Decision tree for German Satellite Data Security Act

not the entire sphere. Studies, such as the GEOHR study by ESA, looked for 100m – 10m geometric resolution with about 1h to 5 min revisit capability. Very advanced technology also looked into Synthetic Aperture Optics, i.e. to deploy a constellation of imaging satellites with a small aperture, but electronically linking them together to create a virtual large telescope (as already done by astronomers with ground based telescopes).

For the time being global and immediate presence with very high resolution satellites seems technically and financially not feasible. Earth Observation based law enforcement (and many other applications) has to live with the current snapshots taken by satellites. A kind "GoogleEarth Live" – and with it all the legal implications – seems currently out of reach. However, applications such as GoogleEarth have shown, that it might need the right "application" or "business case" to possibly make this a reality in future.

2.3 The Disaster Charter and Highlighting Issues of Haiti Earthquake

by Atsuyo Ito

2.3.1 Introduction

The massive earthquake that struck Haiti on 12 January 2010 shook the whole world. The scale and impact of the disaster, coupled with the vulnerability of the nation, which is said to be the poorest nation of the Western hemisphere, was appalling. The affected population is said to be over 3 million and the estimated death toll is over 230,000. Many governmental and public buildings were severely damaged or destroyed – including the Palace of Justice, the National Assembly, the Supreme Court, Port-au-Prince Cathedral, and National palace. Vital infrastructure necessary to respond to the disaster was severely damaged, such as the collapse of UN peacekeeping in Haiti, and the serious damage to the control tower at the international airport and to the sea port. A number of satellite data and derived products have been provided free of charge to afflicted states under the framework of the International Charter on Space and Major Disaster (hereafter: the Disaster Charter).[3] Having been successfully operating for a decade, and this time following the Haiti earthquake, the partners of the Charter provided Haiti critical information to respond to disaster (e.g. map of affected areas, and damage assessments of infrastructure including governmental buildings, hospitals, roads and bridges). Despite such useful knowledge, the victims outnumbered the aid provided. The Haiti earthquake shows how massive disasters could devastate and paralyse the central government of afflicted states to respond to disasters, and require further assistance and intervention by external parties. Whilst the sovereignty of afflicted states should be respected, actions beyond the sovereignty may be necessary to maximize the rescue and relief efforts under the extreme circumstances. This paper undertakes the case study of the Haiti earthquake, highlights the issues of disaster response associated with the Haiti earthquake, and discusses possible improvements that can be brought by the Disaster Charter.

2.3.2 The Background of the Disaster Charter

The Disaster Charter was initiated by European Space Agency (ESA) and Centre National d'Etudes Spatiales (CNES) following the Third United Nations Conference on the Exploration and Peaceful Use of Outer Space (UNISPACE) III conference in 1999.[4] It was signed on October 20, 2000 and has been operational since November 2000. The Charter now embraces six member space agencies, namely, CNES, ESA, Canadian Space Agency (CSA), National Oceanic and Atmospheric Administration (NOAA), Indian Space Research Organisation (ISRO), Comisión Nacional de Actvidades Espaciales (CONAE), the United States Geological Survey(USGS) on behalf of US partners, namely, Digital Globe and GeoEye, the British National Space Centre (BNSC/UKSA) acting on behalf of the international Disaster Monitoring Constellation, and the China National Space Administration (CNSA). There also other non-partner organisations serving as intermediaries. In response to authorized requests, the Charter partners provide data from their satellites free-of-charge to the states affected by natural or man-made disasters.

The Disaster Charter provides a mechanism to make critical space assets available to communities affected by disasters. In response to authorized requests, the Charter partners provide data from their satellites free of charge to the states affected by natu-

[3] "Charter on Cooperation to Achieve the Coordinated Use of Space Facilities in The Event Of Natural or Technological Disasters."Rev.3 (25/4/2000).

[4] UNISPACE is a UN organised international meeting where UN members and space agencies gather. At UNISPACE III the use of space technology for solving regional and world problems was discussed along with the need for international cooperation and use of space applications among developing countries.

ral or man-made disasters[3]. The afflicted states can use the data to monitor their disasters, assess the course of the disasters, and then respond to the aftermath of these disasters. The Disaster Charter is innovative in that it has established a mechanism of cooperation amongst the disaster community worldwide as well as to provide the service completely free-of-charge to all the afflicted States.

2.3.3 The Scope of the Disaster Charter

Amongst the different stages of disaster management - ranging from mitigation, preparedness, response and recovery[5], the Charter is dedicated for a response phase. However, looking closely at the scope of the Charter, the operations to prepare for disaster are not expected of the partners. Article I of the Charter stipulates " The term 'crisis' means the period immediately before, during or immediately after a natural or technological disaster, in the course of which warning, emergency or rescue operations take place"[6] It is clear that early warning or risk assessment to mitigate the disaster falls outside the scope of the Charter. Although the definition 'period immediately before' does not exclude the possibility of the Charter activation for the purpose of pre-disaster warning, in reality the Charter has never been activated in such a way prior to a disaster. Hence, the Charter takes a post-disaster approach: it does not prevent certain (preventable) disasters from happening but it mitigates the impact of the disaster once it has occurred.

Not all the disasters are subject for activation of the Disaster Charter. Disasters excluded from the scope of the Charter are: war, armed conflicts, humanitarian actions not linked to a specific disaster, droughts, and routine epidemiological outbreaks. Furthermore, it cannot be activated for non-emergency situations such as oil spill, and ice monitoring except for specific events. It needs to be stressed that generally calls beyond the emergency period, a Charter activation occurring more than 10 days after the actual crisis start should be rejected. One can conclude that the Disaster Charter is limited to the urgent disaster situation that benefits from the monitoring from the satellite.

2.3.4 The Mechanism of the Disaster Charter

The unique feature of the Disaster Charter is that the Charter partners – providers of data - cannot initiate the process. It is the Authorized Users that can request the activation of the Charter. Authorized Users, after the request for the Charter activation is processed, hand over the operation to a project manager who becomes responsible for the whole course of operation: tasking of satellites, acquiring and delivery of data. The whole operational cost of Charter activities in acquiring the satellite image, processing the data and even producing derived products is to be covered by the partner space agencies. Article 3.1 of the Charter stipulates that "the parties shall develop their cooperation on a voluntary basis, no funds being exchanged between them".[7] Thus, the Charter service is provided voluntarily. Its concept is based on goodwill and best endeavours. The Charter is not a binding instrument embodying parties with full legal duties and obligations. Rather it incorporates agreements expressing the intention of cooperation between the space agencies to assist the afflicted states.

The process of the Charter activation is complex. There are several ways to activate the Charter: 1) direct activation; 2) activation via an Authorized User on behalf of a user from a non-member country (activation via sponsored AU); 3) activation via the UN for the UN users; 4) activation for Asia pacific users via Sentinel Asia's partner, the Asian Disaster Reduction Centre. Now the channels for Charter activation have broadened compared to the early operational periods. Combined with the similar disaster response mechanism, such as Sentinel Asia, the Charter increasingly serves more areas around the globe. A brief explanation for each is provided below.

Direct activation is the activation by Authorized Users such as the civil protection and the relief agencies of the countries whose jurisdiction cover the member space agencies. Authorized users are the only bodies authorised to request the services of the Charter for a disaster occurring in their country or territory.

Whilst most cases an Authorised User request the Charter activation to help its own country, activation to may request the Charter to assist a disaster management user from another country in response to a major emergency. For example, activation requests from users in Latin American countries are often

[5] Holloway R., "Is Space global disaster warning and monitoring now nearing reality?" 17 Space Policy (2001): 128.
[6] "Charter on Cooperation to Achieve the Coordinated Use of Space Facilities In The Event Of Natural or Technological Disasters." Rev. 3 (25/4/2000). Art. 1. Last visited: 23 June 2010 <http://www.disasterscharter.org/web/charter/charter>.
[7] Art. 3.1, "Charter on Cooperation to Achieve the Coordinated Use of Space Facilities In The Event Of Natural or Technological Disasters." Rev. 3 (25/4/2000). 24 June 2010 <http://www.disasterscharter.org/web/charter/charter>.

submitted via the Argentinean Authorised User. This is referred as activation by a sponsor Authorised User.

The third one is activation by the UN. The Charter has an agreement with UN OOSA (Vienna) and UNITAR/UNOSAT (Geneva) to provide support to UN agencies. UN OOSA and UNITAR/UNOSAT may submit requests on behalf of users from the United Nations. Since the UN has a global presence, it is particularly useful to activate the Charter for countries that are not familiar with the Charter operation – for example, the Charter activation by the UN is taking place in several African countries.

An option for the Charter activation is now open to Asia Pacific users via Sentinel Asia's partner, the Asian Disaster Reduction Centre. Sentinel Asia is a disaster response mechanism similar to the Disaster Charter based on regional collaboration for Earth Observation based emergency response in 31 Asia Pacific countries. Since 2009 the Charter has granted the Asian Disaster Reduction Centre the right to request for the Charter activation on behalf of Sentinel Asia users. Thanks to this established link, Asian countries have improved access to space assets.

It is worth noting furthermore that coordination is under way with Group on Earth Observation (GEO). In response to a request from the GEO to improve access to the Charter during emergencies, collaboration has started with primary focus on users from African countries that do not have a direct access to the Charter.

In these ways, the target for imaging is the whole globe and the parties concerned in the operations Charter is taking steps toward the covering different regions of the world through different channels.

2.3.5 The Legal Environment of the Disaster Charter Regarding the Principle of Sovereignty

The Disaster Charter based on the remote sensing from space allows that observation of the afflicted state could take place without the request by the afflicted states. Sensing from space is completely permissible under the international space law as imaging the afflicted state is based on the freedom of outer space established by the 1967 Outer Space Treaty[8] and 1986 UN Remote Sensing Principles.[9] Principle IV of the UN Remote Sensing Principles stipulates that "Remote sensing activities shall be conducted in accordance with Article I of the Outer Space Treaty"[10], which establishes the free use of outer space. Therefore, the UN Remote Sensing Principles establish the right of observing the entire globe from outer space. Whilst the Disaster Charter is activated following the request by the afflicted states if disasters hit the countries of the Charter partners, in case disasters that hit countries other than the Charter partners, activation is most likely to take place by a sponsored authorized user, the UN, that is parties other than the afflicted states.

2.3.6 The Impact of Charter Operations from the Standpoint of Disaster Response

Due to the legality of satellite remote sensing based on the Outer Space Treaty and UN Remote Sensing Principles, the Disaster Charter allows the provision of data to any afflicted State providing any of the above designated process to request the Charter service is followed. This has a significant impact on the effectiveness of disaster response, which fundamentally follows the humanitarian principle, that is, aid is provided upon the request of the afflicted state. A brief analysis of a nature of disaster response warrants a discussion here.

Disaster response is governed by the principle of sovereignty. Article 2.7 of the UN Charter state that "Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter...".[11] The principle of territorial sovereignty also applies to disaster situations such as international aid from abroad. The fundamental principle for disaster response is that it is for afflicted states to decide whether to request and accept international assistance in case of a disaster.[12] Hence, it will not be considered unlawful if the afflicted State do not request for assis-

[8] *Treaty* on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, London/Moscow/Washington, done 27 January 1967. Entered into force on 10 October 1967, 610 UNTS 205, 6 ILM 386 (1967) Hereafter: the Outer Space Treaty)

[9] United Nations General Assembly. Principles relating to remote sensing of the Earth from space. GA 41/65 of 3 December 1986. (Hereafter: the UN Remote Sensing Principles)

[10] Ibid. Art. IV.

[11] Art. 2.7, United Nations Charter. Entered into force 26 June 1945, in San Francisco.

[12] United Nations General Assembly. Strengthening of the coordination of humanitarian emergency assistance of the United Nations. Annex I.3. "humanitarian assistance should be provided with the consent of the affected country and in principle on the basis of an appeal by the affected country." GA 46/182 of 19 December 1991.

tance or even refuse to accept international assistance. This allows for a high degree of discretion by governments in disaster response, despite the imminent needs.

2.3.7 Politics Involved in Disaster Response

There are occasions when, strictly for political reasons, affected states have actually refused the aid offered from foreign governments. Major example includes the Indian Ocean Tsunami in 2005 and Cyclone Nargis that struck Myanmar in 2008. Following the Indian Ocean Tsunami, India refused to accept any foreign aid denying the access of NGOs to the Andaman Islands, partly because of the presence of a key military base on Car Nicobar Island.[13] Likewise, following the Nargis Cyclone, the military government of Myanmar refused international aid for weeks, resulting in unnecessary loss of life. In these ways, politics can have a disproportionately negative impact on disaster response and relief operations.

The fact that Charter can be activated without the consent of the afflicted states has an important implication for disaster response. It means that affected areas of the territory of afflicted State can still be imaged regardless of the state of the affected State - even the government takes the reluctant stance to call for humanitarian assistance outside that State or the government is incapacitated to respond. The Charter operations based on satellite remote sensing partly overcomes the initial stage of a hurdle of the principle of State sovereignty governing disaster response as it would permit getting the overview of the afflicted State without their consent. The further stage, that is, when the territorial sovereignty comes to the issue, would involve the domestic response to actually rescue survivors and provide relief. The next part discusses how response to the Haiti Earthquake was slow and how improvements can be brought by the Disaster Charter.

2.3.8 Slow Response Experienced in the Haiti Earthquake

The striking feature of the Haiti earthquake is that it struck the capital and devastated the major functions of the government. Historically, few disasters had such effect. One can only name the Great Kanto Earthquake of magnitude 7.9 that struck Tokyo in 1923 as the one comparable to the Haiti earthquake.

In addition to the governmental buildings, bodies to respond properly to the disaster were severely affected. For instance, despite of the 9,000 peacekeepers stationed at UN Stabilisation Mission Haiti (Hereafter:MINUSTAH), initially none of them appeared to be involved in hands-on humanitarian relief in what emergency medical experts describe as the critical first 72 hours after the disaster as they were affected themselves[14]. Instead of helping the Haitian affected communities, they were involved in the search for survivors at the collapsed headquarter of MINUSTAH.

Completely overwhelmed by the scale and extent of disaster, Haiti was compelled to rely largely on aid from abroad. Donations were made from many states abroad. Around 26 international search and rescue teams arrived to Haiti.[15] A major leadership was displayed by the US - since the control tower of the International airport of Port-au-Prince has collapsed, the Haitian government formally put the airport's operation in US hands and Washington has established a temporary air traffic management system for flights[16]. However, the impact of the disaster resulted in the situation that absence of effective 'control tower' for the disaster response at large – uncoordinated actions and efforts were taken at least by Haitian, aid groups and the US.

Haiti President Rene Preval criticised the lack of coordination amongst the countries that have come forward to assist victims[17]. A problem of coordination already started at the airport. A cargo plane by aid group, Médecins sans Frontières, which carries medical equipments were turned away from landing at Port-au-Prince airport by the US[18]. Relief operations were chaotic as there was confusion as to who were in charge. The situation resulted in the delay in providing the relief and caused the angry appeals from the survivors and looting on the street.

2.3.9 The Issues Raised by from Haiti Case with Respect to the Charter

The parties concerned in the operations of Disaster Charter were quick to respond to

[13] Lepp, N. "Disaster Relief Politics Complicate South Asia Effort." The Dominion, 3 Jan. 2005: 1.

[14] Brown, T. "Haiti aid effort marred by the slow UN response." Reuters Alertnet, 26 Feb. 2010. <http://www.alertnet.org/thenews/newsdesk/N25200825.htm>.

[15] "Logistical nightmare hampers aid effort." BBC News. 22 Jan. 2010. <http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/americas/8460787.stm?ad=1>.

[16] Ibid.

[17] "Haiti President Criticises Lack of Coordination in Quake Relief Measures." <http://www.india-server.com/news/haiti-president-criticises-lack-of-20208.html.>

[18] Tran, M. "Aid plane turned away from Haiti airport, says medical charity." Guardian 17 Jan. 2010.

Haiti earthquake. The Charter activation was requested by French Civil Protection, UNOOSA on behalf of UN Stabilisation Mission in Haiti (MINUSTAH), Public Safety of Canada, American Earthquake Hazards Programme of USGS. Under the framework of the Disaster Charter, satellite imagery was provided on 14, which is 2days after the catastrophe. A number of products such as a map of affected areas with different magnitude of damage, and damage assessment of different infrastructure, were provided to end users. On the other hand, it needs to be stressed that the Charter operation is primarily designed for national experts to plan relief operations and to give the direction of aid. The essential purpose of disaster response is of course, rescue and relief of survivors, and therefore, the key to the success of Disaster Charter ultimately hinges on how much the satellite data provided can be utilized effectively to facilitate relief efforts. If the government is not in a state to respond, supply of satellite images would not lead to enhanced relief efforts. Even if the users external to the afflicted state receive products, it needs to be used to implement the relief operations inside the territory of an afflicted state. The first step is of course that affected areas are imaged and obtained data are provided to afflicted states, however, under the exceptional circumstances as the Haiti Earthquake, victims would have benefited from further steps. Further steps would involve decision making for disaster response - planning relief operations and to give the direction of aid, and of sending relief workers on behalf of the government.

It is not desirable that such decision and direction of aid be taken by all of the aid groups and countries that have come for help at their discretion. Such a situation would generate even further chaos. A similar situation was just as experienced by the Haiti Earthquake. The domestic 'command centre' for disaster response was seriously impaired if not absent, and coordination lacked amongst the operations undertaken by various actors involved. The linkage between 'on the site operation' and knowledge on the affected areas is essential to avoid overlapping operations and cover all the areas in need. The parties engaged in the Charter operations have the good knowledge for the aftermath of the disaster, both the overview and site specific details. They are most likely to be more familiar with the overview than the workers on site and decision makers in Haiti. Hence, the parties engaged in the Charter operations are in a highly suited position to coordinate and give direction of aid. They would be competent to prioritize the areas to serve in accordance with the degree of severity of damage, and finding passable routes to reach the affected sites. The extended role that can be played by the parties engaged in the operations of the Disaster Charter is considered highly beneficial.

2.3.10 Conclusion and Recommendation

The Charter operation is working so successfully and has the potential to contribute even more to the exceptionally devastating disaster situations. Haiti experienced the extreme level of chaos and devastation that actions beyond simply delivery of satellite products to end users deemed necessary. There is a need for external intervention in case the government affected by the disaster is unable to respond properly. Options need to be considered for the parties engaged in the Charter operations to take further steps to intervene and organize the relief efforts. The Charter partners and associated bodies could serve as a decision making body in place of a severely affected government and should be given a mandate of coordinating the relief efforts so that they can actually send personnel and providing aid supplies to the sites.

However, this is only possible with the will and consent of the afflicted states. A mechanism should be available for all states to accept the good will intervention for disaster response at a domestic level under the extreme circumstances. It is recommended for afflicted sates to relax the application of territorial sovereignty to promptly allow relief. It is recommended that there should be a prior arrangement amongst the states to authorize the Charter partners or other authorized agencies to direct, and send aid and rescue personnel to the affected population. Such an arrangement could be realized by the sign-up by the willing states - states would sign up in times of peace assuming for such extreme circumstances. If the states that have signed up are struck by deadly disasters, afflicted states could benefit from the hands on operations by international or foreign rescue teams without their request at the immediate aftermath. It is proposed that direction of coordination such as assigning roles/tasks to different aid groups should be undertaken by the project manager of the Disaster Charter or others who are best familiar with the state of the aftermath.

Whilst statistically, the possibility that a disaster strikes the capital and incapacitates an infrastructure to respond is not high, one can never predict where the disaster strikes. It is hence necessary to envisage all conceivable scenarios and prepare for them. Scenarios cannot completely rule out the risks of the deadly disasters hitting the capital of any

state and then destroying the significant infrastructure for disaster response. In such circumstances, arrangements to facilitate international assistance inside the territories would contribute to minimize victims of disasters.

2.4 Use of Satellite Data for Treaty Monitoring

by Jana Jentzsch

Verification provisions in international agreements have strongly influenced the development of international law through the last decades. Important disarmament negotiations have failed because there was no consensus on the verification regime. Other treaties gained international acceptance only because its verification provisions were strong and fostered international collaboration and understanding, such as the bilateral SALT agreements between the USA and the former USSR. The 1993 Chemical Weapons Convention (CWC) comprises the most elaborated verification regime ever agreed upon and it is the first treaty that aims at the entire destruction of one type of weapons of mass destruction.

2.4.1 Definition: What Is Verification?

Before considering the role of satellite imagery in treaty verification, It needs to be clarified what exactly the term verification means, in which context it is used and which types of connotations it may imply.

Verification can be defined as the process by which compliance or non-compliance with an agreement is determined. Verification can detect non-compliance, deter parties which may be unable or unwilling to comply and provide compliant parties with the opportunity to demonstrate explicitly their compliance (so-called confidence-building measures). Verification also provides reassurance to all parties that the overall implementation of an agreement is proceeding effectively and efficiently. Although there can never be a total assurance that all parties to an agreement are complying with all of its obligations, verification supports a reasonable level of certainty that cheating can and will be detected. Early detection is essential so that other parties can take suitable action, ranging from simply asking the suspected party for clarification to the imposition of some sort of sanction or even treaty withdrawal. Sanctions according to Chapter VII of the UN Charter may consist of diplomatic measures, economic penalties and military action.

According to a wider understanding, verification also comprises the ascertainment of facts that are otherwise important in the relationship between certain states. An ascertainment of facts as a dispute settlement procedure can become important in the context of peace missions, during treaty negotiations and in the context of international judicial proceedings. Peace missions need to be based on a specific authorisation. However, this is often not a multilateral treaty, but rather a mandate by the United Nations or other international organisations like NATO or OSCE. Such mandates do not necessarily constitute binding international treaty law.

2.4.2 Verification and Monitoring

Verification permits the parties to an agreement or mission to determine whether they are complying with their obligations. This if often confused with the term “monitoring”. However, the latter refers merely to the technical process of information gathering for a concrete purpose, while it does not relate to the compliance judgment. Monitoring refers to efforts of detecting, identifying, and measuring developments and activities of interest. Therefore, “treaty monitoring” refers to the technical process of information collection whereas “verification of treaties” refers to the legal process of both the observance process and deciding about its results.

The process of verification can be divided into three major (and chronological) steps:

- Collection of relevant information (“monitoring”),
- Information assessment which is supposed to end with a verification judgment, and
- In case of a detected violation: adequate reactions.

Satellite remote sensing is only one specific tool of verification capabilities. The advantages of this means of verification become quite evident if one looks at the results of present technological and economic developments.

In the past, verification was associated mainly with arms control and disarmament but in the course of the years it has been practiced in other areas as well, for instance in the framework of monitoring peace agreements and environmental treaties, and also in watching human rights. In each of those areas, the importance and role of verification is different.

2.4.3 Disarmament and Arms Control Treaties

Maybe nowhere else verification is as crucial as in international disarmament and arms control –but also most difficult. In no other area states are as concerned about their sovereignty as in this field where national security and sensitive information are at stake.

The history of satellite data in the verification process of disarmament and arms control treaties is long. Here is a short overview of the most important treaties:

- bilateral arms control and disarmament treaties of the cold war (SALT I, SALT II, ABM Treaty);
- multilateral nuclear test ban verification (Limited Test Ban Treaty LTBT, Comprehensive Nuclear Test Ban Treaty CTBT *(not yet in force)*);
- multilateral nuclear non-proliferation verification (Nuclear Non-Proliferation Treaty NPT);
- anti-chemical weapons verification (Chemical Weapons Convention CWC);
- anti-landmines verification (Ottawa Convention).

The bilateral SALT agreements between the USA and the former USSR of the 1970s were the first treaties that introduced rules which were verified with remote sensing satellites. The verification missions during the cold war era were conducted merely by strictly national technical means. The satellites were operated unilaterally by one party and no international control took place. The national satellite capabilities were capable to detect missile launchers, but in the early years delivery systems were often impossible to discover. As a consequence, satellites used as National Technical Means (NTM) helped freezing the number of strategic missile launchers, but not of delivery systems.

The subsequent multilateral disarmament treaties of the 1980s and 1990s also do not contain explicit provisions to use satellite data as international technical means of verification. However, these treaty regimes, especially the CTBT, the NPT and the CWC, provide for stronger general verification provisions and states parties may use gathered satellite data as evidence in evaluation processes of the international treaty organisations, such as the OPCW (Organisation for the Prohibition of Chemical Weapons) for the CWC or the IAEA (International Atomic Energy Agency) for the NPT. In fact, the use of satellite-based monitoring technologies is widely accepted and applied. In particular, the OPCW in The Hague uses satellite data in the framework of its well elaborated system of international verification. Also, commercial satellite data may be used as a supportive tool in the verification process. For instance, while the CTBT and its international monitoring system exclusively rely on “post test” technologies to reveal nuclear test explosions that already occurred, commercial satellite imagery may be used to detect “pre-test” as well as “post-test” activities. Watching sites for potential nuclear test preparations –which are not covered by the CTBT-, is significant as the threshold from allowed to illicit activity is small and difficult to determine. Satellite imagery may give rise to start directing the work of the CTBT to a certain site.

Also, nuclear facilities in suspected proliferant states have frequently been identified by satellite imagery, including high-resolution commercial satellite imagery, although the analysis often includes information from other intelligence sources or the IAEA directly. Satellite imagery is able to identify a nuclear weapon production facility. Multiple images may prove progress in the construction of a facility and increase in the number of buildings at a site. Annotated images may monitor the intrusive verification requirements of the NPT. Furthermore satellite data can contribute to historical assessments of nuclear programs in proliferant states. Unfortunately, the recent NPT review conference in May 2010 did not bring concrete results with regard to the further development of satellite-based treaty verification.

2.4.4 Environmental Protection

In the course of the last 50 years there has been a striking multiplication in the number of multilateral environmental treaties. More than 210 environmental agreements are listed by the United Nations Environment Programme (UNEP); more than 200 of those were adopted after 1951 and approximately 75 % of these were agreed upon after the 1972 UN Conference on the Human Environment in Stockholm. Though, when environmental protection is at stake, binding treaties and strong verification provisions are still relatively rare. Most environmental agreements do not contain any specific reference to verification. However, some of the very new accords do provide for some necessary elements: instead of developing a specific set of rules in an annex or the accord itself, verification is implicitly contained in a wider system for implementation review. For example, the Kyoto Protocol to the United Nations Framework Convention on Climate Change attaches great relevance to research and development and the establishment of obser-

vation systems. Article 10 (d) of the Protocol stipulates:

> » All Parties […] shall co-operate in scientific and technical research and promote the maintenance and development of systematic observation systems and development of data archives […].

Respective obligations for the need of observation of greenhouse gases and the review of the implementation of the Kyoto Protocol are also mentioned in its Articles 7, 8 and 13. Still, satellites used for assessing climate change often suffer from insufficient reliability. Some of it concerns the calibration of hyper-spectral sensors mounted on the satellites, which measure various parameters from average global temperature to aerosol presence in the troposphere. In particular, the calibration of sensors is very sensitive and can easily be damaged during the launch process.

2.4.5 International Conflicts, Peace Missions & Agreements

Space-based assets should be used to enhance international security in an ongoing way, regardless of any treaty establishing concrete obligations to be monitored or if other events threaten international peace and security. International peacekeeping operations, most prominently conducted by the UN, but also by other organisations such as NATO, have taken place in various states in the past decade. These were mostly civil wars or the existence of inhuman dictatorships which urged the international community to intervene.

In the future remote sensing techniques with its highly capable 24-hours means of observation may make it possible to support or even replace the military human observer. The progress in aerial and space observation may allow the development of more capable and less intrusive means of mechanical monitoring. For example, satellites monitoring dangerous frontiers, cease-fires, or weapon storage sites could replace human presence. An important role for satellites in international conflicts may also be the combat of piracy and protection of maritime security.

In addition to remote sensing satellites, access to the navigation system GPS has been made widely available for peacekeeping missions. With the help of GPS, peacekeepers can determine the precise location of ceasefires and territorial frontiers, as well as their own exact positions when on patrol or based in abandoned areas. With GPS, the users are also able to easily communicate this information with their headquarters or other peacekeeping forces. The European Galileo system will presumably provide similar services.

2.4.6 Human Rights

Contemplating international and regional human rights instruments, one can easily discover specified rights, but rarely provisions specifically designed for an organized control, for a verification of the rights. This task is generally upon the various UN human rights offices, above all the UN Human Rights Commission and the High Commissioner for Human Rights but also on many specialized bodies, and regional institutions, especially courts. The General Assembly is empowered under Article 13 of the UN Charter to initiate studies and make recommendations regarding inter alia human rights. Such studies frequently deal with alleged violations of certain states.

Apart from the UN and regional courts, it is mainly non-governmental human rights organisations which autonomously try to verify human rights with their best efforts. They issue reports on topics such as torture, rape, racial discrimination, attacks against minorities, labour rights or women's and children's rights. The civil efforts of NGOs such as Human Rights Watch, Amnesty International, or Landmine Monitor, are a precious tool for verification, as they raise public awareness and may even initiate actions from governments or international organisations. Satellite data will increasingly support such efforts, as the available resolution is continually increasing, and certain types of abuse (e.g. the burning of villages) have already become detectable.

2.4.7 Conclusion

Although often not sufficient by itself, satellite imagery already constitutes a major tool for the verification of international obligations and the strengthening of international security. The fact how international obligations can be verified also determines the credibility and effectiveness of the respective agreement or obligation. Through the adoption of intrusive verification provisions, which e.g. also provide for challenge inspections in cases of serious suspicions, the motivation and ratio of member states to adhere to the agreement can be increased. Satellite imagery should be explicitly mentioned in the respective treaties, agreements and mandates, as international verification institutions should not have any doubt that they can decide about ordering imagery from commercial sources.

Yet, the negotiation of international treaties in general and verification regimes in particular strongly depend on political will and intent. International law always is codified international policy and when drafting new rules legal scholars need to consider the realities of international relations. Although, in the past decade, international lawyers needed to recognize that organized treaty verification cannot be considered as an ongoing success story anymore. After September 11, 2001, in particular the United States administration has pursued a policy of strong suspicion against binding international agreements. In consequence, the further strengthening and development of international verification provisions did not take place. Still, the international legal community should continue to promote the need for clear verification provisions and the integration of satellite imagery into the respective verification regimes.

2.5 Satellite Data and Applications for Law Enforcement Purpose

by Jean-François Mayence

The idea of collecting information about others is certainly not new. It is likely that, in every organized society in every civilisation of the human history, human leaders have been aware of the need to manage such information in order to establish their sustainable power. The content of the information itself has not changed much through the centuries: answers to basic questions such as *where is he/she? where is he/she heading? what is he/she doing? who is he/sheet meeting?* etc., were the keys for natural deductions and further, the elaboration of an appropriate (counter-)strategy.

The technological possibilities provided by the satellite systems have just dramatically multiplied the scope, the accuracy, the amount and the availability of information we might need in order to deal with a specific situation. With satellites in orbit collecting information on any place, at any time, we start dreaming about *omniscience*. But this dream is also a nightmare: the idea of being watched, of being searched without even realizing it, is a deep cut in our privacy.

At this stage of the development of the so-called "Information Society", a sound reflection seems necessary about the thin line between the reality and the phantasms, between the wishes and the fears, and most of all, about the place of law in such a development. Can the expansion of our knowledge and our technical means modify our basic values, those which are supposed to be protected by the rules that our society adopts and implements?

2.5.1 Satellite Applications

From an user's point of view, technical means do not really matter as long as the information remains accurate and reliable. All he eventually gets are the elements of information on which he will be able to base his action. Therefore, even if we know that each domain of satellite applications (telecom, positioning / navigation, observation) is subject to its own rules, the origin of the information is not necessarily relevant in defining the legal regime applicable to its use.

Law enforcement, in the broadest meaning of the term, is aiming at making law a reality wherever and whenever a legal settlement is required in order to solve a conflictive situation. It is based, first on the establishment of facts, in order to allow an appropriate response from any party affected by the situation, then on the provision of legal evidences, possibly based on the said facts, to allow an authoritative ruling. This second phase (the provision of evidence) is certainly the most interesting from a legal point of view since the admissibility of the evidence requires the satisfaction of several criteria, among which the compliance with the rule of law. It is a general principle commonly recognised that no evidence can be brought on the basis of a breach of law[19]. In certain cases, the law itself imposes a certain form of evidence exclusive of any other (contractual law, real estate law, etc.)

The whole reflection on the legal aspects on the use of satellite applications and data should therefore concentrate on securing the legal validity and the compliance of such a use with respect to the applicable rules (notably the protection of privacy, the protection of sensitive information, the non-discrimination principle), but also, in a more positive way, help satellite service providers with adjusting their products in order to meet the potential demand of law enforcement authority and to convince them to consider satellite applications as a tool in the implementation of their mission.

[19] This statement must of course be nuanced with regard to particular applicable rules according which, in certain cases, the irregular origin of the evidence doesn't affect its validity.

2.5.2 Use of Satellite Data and Applications for Law Enforcement Purpose: Non-Judicial Procedure

A large number of legal instruments (laws, regulations, conventions, agreements, contracts) requires the continuous, periodic or casual monitoring of particular situations. In this case, no judge is involved: it remains between a public authority and the persons subject to it, or between two or more contractors. In this context, it is up to each instrument to determine, explicitly or implicitly, the value that can be recognised to the use of a particular method of monitoring. Here, the admissibility of the information brought by the satellite is in principle not to be questioned. This issue is rather focusing on its accuracy and its technical reliability.

Environment law is certainly a domain where satellite applications are recognised as important monitoring tools. It is the case whenever the surveillance of a particularly wide or remote area is at stake: agriculture law, Antarctic law, maritime law[20], etc.

Contractual law is characterized by its flexibility which allows parties to provide for the use of the means of their choice for the monitoring of their respective obligations. Nevertheless, the recourse to new technologies has often a deep and broad impact on the whole economical sector.

Another area of law which might be heavily impacted by the use of satellite applications is the transport sector. In particular, maritime law is based on rules inherited from very ancient legal institutions which have survived until today. But the satellite era might cause a revolution which would put an end to them, notably through the notion of *Embedded Eye*[21], as highlighted by Prof. Dr. Jacques Libouton at the occasion of the Belgian Senate's Colloquium on Legal Aspects of Space Activities and Space Applications, held in Brussels on April 26, 2006[22].

The whole economy of maritime freight transport and, by extension, of combined transport, is based on the idea that it is almost impossible to know, at a given moment in time, where the transported goods are exactly located and in which condition they are. Furthermore, maritime transport has always been subject to particular risks and this uncertainty on the good delivery of the freight has become a part of its value. Finally, considering the time taken by long-distance shipping (even though considerably reduced by modern transport means), traders have invented new form of trading based on documents representing the goods during their transport. In close connection with the sale itself, other operations have become usual and part of the business: credit, insurance, etc. An excellent example is the integration of the maritime *alea* in the specific insurance contracts. Contrary to general insurance law, maritime insurance covers, in certain conditions, the *potential risk,*[23] namely the risk that would have already occurred at the time of the conclusion of the insurance contract, if it is demonstrated that none of the parties would have known about this occurrence. It is obvious that such provisions would be deemed obsolete with the use of satellite tracking allowing a quasi-real time information on the freight, on its location and its status. With the panoply of sensors nowadays, any relevant information needed for the trading of the freight can theoretically be available in real time. By embarking optical camera or sensors able to determine the chemical composition of the air onboard a container, or the shocks that the goods have undergone, and by transmitting this information to the charterer or to any other interested user, the value of the freight can be updated on demand, taking into account of its actual position on the route.

We will not extend our study of the use of satellite data for surveillance and treaty monitoring since this topic is widely reviewed by other articles in this publication. But we can nevertheless point out the main other domains of application of satellite surveillance:

- disarmament and weapons control (see notably the use of satellite data expressly mentioned in the framework of the CTBT/CTBTO)[24];

[20] Apart from the *Song San Ship* case which led to a judicial procedure and which therefore will be reviewed in the next section, another incident was observed by satellite in October 1997 in Singapore. A very large crude carrier and an oil tanker collided and spilled about 28,000 tonnes of oil, comparable to the amount in the Exxon Valdez spill, into the sea. Clean-up operations were very successfully carried out, with nearly all the spill enclosed and cleaned up within a few days. ERS and RADARSAT images acquired 5 days and 10 days after the collision showed some residual oil slicks drifting north-westward along the Malacca Straits. It is likely that such observation contributed to mitigate the damage.

[21] Libouton, Jacques. "Space Applications and Transports." European Transport Law. 2006. 479.

[22] Belgian Senate's document. Session 2005-2006, 3-1785/1 <http://www.senate.be>.

[23] Art. L172-4, Code des Assurances. France; Art.6.1, Maritime Insurance Act Art. 219, Code de Commerce. Belgium. Livre II, Titre VI, Section 2.

[24] Art. IV, A, par. 11, Comprehensive Nuclear-Test-Ban Treaty. Done on 24 September 1996. New York (not yet entered into force as on June 1, 2010 but actually implemented through the CTBTO, its International Monitoring System and its International Data Centre)..

- fisheries activities management[25];
- agriculture regulations enforcement[26];
- real estate.

Beside of surveillance purposes, the satellite may also be used for global management. This is the case, for instance in the following areas:

- health monitoring at global scale, epidemiology[27], health insurance statistics;
- food security[28];
- land management.

2.5.3 Use of Satellite Data and Applications for Law Enforcement Purpose: Judicial Procedure

In the context of a judicial procedure, things are a little bit different. In addition to the technical reliability requirements, specific legal rules need to be taken into account. The admissibility of the data as a legal evidence or an element of legal evidence will be subject to the applicable law governing the procedure: civil, commercial, criminal... People in charge of enforcing the law are themselves subject to the law and their compliance to the rules will be a condition of the admissibility of the data by the judge.

In a contractual relationship, the parties are free, to a certain extent, to determine the means of evidence applicable to the supervision of the execution of their commitments. Even when no specific technical means is mentioned in the contract, satellite observation might provide a legitimate source of information on the execution of each parties' commitment. This was for instance the case with the agreement signed between the Belgian State and the International Polar Foundation on the construction of the Belgian Princess Elisabeth Antarctic Polar Station: the progression of the work and the functioning of devices such as wind turbines were monitored by satellite (high-resolution pictures from military satellites). Even though no judicial settlement was ever necessary in this case, it is likely that satellite observations could have served as elements of evidence for the enforcement of the agreement.

Another illustration is provided by Employment Law. The use of a positioning system seems to expand as a new trend in order to locate workers and to subject them to a continuous surveillance. The legal response may of course be different from one country to another: the United States have already developed some case law about this issue. In *People v. Weaver*[29], the administrative law

[25] Molenaar, Erik Jaap, Tsamenyi, Martin. "Satellite-Based Vessel Monitoring Systems (VMSs) for Fisheries Management. International Legal Aspects and Development in State Practice". FAO Legal Papers Online 7 Apr. 2000. <http://www.fao.org/legal/prs-ol/lpo7.pdf>

[26] Macrory, Richard. "Satellite Monitoring as a Legal Compliance Tool in the Environment Sector". Arts and Humanities Research Council Report 2. <http://www.ucl.ac.uk/laws/environment/satellites/docs/2_AHRC_Agriculture.pdf>

[27] World Health Organisation's activities. <http://www.who.int/health_mapping/about/en/>. European Space Agency's programmes. <http://www.esa.int/esaEO/SEMY8G3VQUD_environment_0.html>. Secunda, Paul M. "A Mosquito in the Ointment: Adverse HIPAA Implications for Health-Related." Remote Sensing Research and a "Reasonable" Solution. Journal of Space Law Volume 30, nr 2, University of Mississippi, School of Law, 2004.

[28] European Commission Joint Research Centre's projects. <http://ec.europa.eu/dgs/jrc>.

[29] State of New York, Supreme Court, Appellate Division, 3rd Judicial Department, June 5, 2008 (12 NY3d 433) - cf. notably "Adjunct Law Professor Blog", report by Mitchell H. RUBINSTEIN:
Facts: A police officer, in the course of investigating a series of burglaries and acting without a warrant, attached a battery operated global positioning system (hereinafter GPS) device under the bumper of defendant's van while it was parked on a public street. The device remained in place for 65 days. Based upon the data retrieved from this device and other evidence, defendant and a co-defendant were arrested and charged with burglary in the third degree and grand larceny in the second degree in relation to a theft from a K-Mart Store, as well as burglary in the third degree and petit larceny in relation to a theft from a meat market six months earlier.
1st degree: No warrant needed: The Administrative Law Judge said that the State of New York Public Employees Relations Board (PERB) has long held that the determination of the type of equipment to be utilized by an employer does not give rise to a bargaining obligation and, accordingly, a balancing of interests test was not appropriate. Further, the Administrative Law Judge found that CSEA's arguments that employees' privacy rights were affected, that they had to participate in record keeping, and that there was an interference with off duty time were either inapplicable or had no factual basis.
2nd degree: Ultimately the issue of the installation of a GPS device without a warrant was addressed by the Court of Appeal. In a four to three ruling, the court ruled that such an action, in this instance, was barred by New York State's Constitution. The Court of Appeals ruled that:
1. The residual privacy expectation Weaver retained in his vehicle, while perhaps small, was at least adequate to support his claim of a violation of his constitutional right to be free of unreasonable searches and seizures.
2. The massive invasion of privacy entailed by the prolonged use of the GPS device was inconsistent with even the slightest reasonable expectation of privacy.
The placement of the GPS device and the ensuing disclosure of Scott's movements over a 65-day period comes within no exception to the warrant requirement, and although the prosecutor did not contend otherwise, the court found the argument that "no search occurred" untenable. The court ruled that the warrantless use of a tracking device is inconsistent with the protections guaranteed by the New York State Constitution noting that technological advances have produced many valuable tools for law enforcement and, as the years go by, the technology available to aid in the detection of criminal conduct will only become more and more sophisticated. "Without judicial

judge denied the necessity to perform a balance of interests test considering that it was the sole decision of the employer and that privacy of the worker was not at stake considering the surveillance was performed in connection with the professional duties. This was overruled by the Court of Appeal of New York which considered that the "residual expectation of privacy" by the worker even during the execution of its professional tasks was sufficient to justify the claim and that such a surveillance should proportioned with regard to the several interests at stake.

In France, the same issue has been dealt with under the provisions of the 1978 Law[30] which establishes the "CNIL" (National Commission for Informatics and Freedoms). Any use of GNSS device in order to monitor the activities of workers in the framework of their professional duties is subject to four conditions:

a) declaration by the employer to CNIL on the use of a GNSS device;

b) information of the worker;

c) proportionality between the purpose of the surveillance and its impact on the worker's interests;

d) deletion of the data at short term (recommendation: 2 months max.).

It is certainly in Criminal Law that the criteria for the use and the admissibility of data collected through high-tech devices have been developed[31]. Those criteria are remarkable and may be considered as an excellent basis of reflection as they provide solutions applicable to various kinds of technologies, from sound capture or sensor-camera's to satellite observation.

2.5.4 U.S. Law

The use of 'scientific evidences' or 'technical evidence' is regulated in the U.S. law at several levels: the U.S. Constitution (IVth Amendment), the Federal Rules of Evidence ('FRE') and the jurisprudence. This latter source is based on a 1923 Supreme Court of the United States case: *Frye v. United States of America*[32] having established the *Frye Test*. The Frye case dealt with the use of the polygraph and the admissibility of this lie detection method as an evidence at court. As a result of the combination of the jurisprudence and the law, such a use of a technical device was considered by the judge under two distinct aspects:

a) the reliability of the method and of its results;

b) the relevance of the collected information with regard to the case.

The *reliability* of the method is demonstrated by its general acceptance by the scientific community and the fact that it is regarded as scientifically valid by most experts, as providing exact and sufficiently accurate results.

The *relevance*[33] of the method can be explained as the recognition of the fact that the method establishes facts in relation with the case, which could not be established with the same degree of certainty by other technical or natural means.

A third aspect could be seen apart from the reliability: the assurance that the results of the method cannot be falsified. This *certifiability* of the results must be distinguished from the reliability to the extent that it doesn't question the general acceptance of the method, but only the specific results on a case by case basis. The issue of certification of data is certainly one of the core issues of the use of satellite technologies for law enforcement purpose. Digital images are considered today as a purely virtual product which is susceptible of manipulation at several stages of its fabrication. Software allows replacing easily one pixel by another and, apart from contractual commitments nothing really exists today in Europe to guarantee the authenticity of satellite data. In the United States, some systems of certification already exists, such as those delivered by the National Climatic Data Centre on weather reports. The need of such certification goes far beyond criminal procedure: actually, any kind of use of satellite data for public or private purpose might require their certification by an independent authority. In Europe, services based on GMES could include the certification of the data provided by a body on a non-contractual basis. Such a reflection has been led in the United States[34].

oversight, the use of these powerful devices presents a significant and, to our minds, unacceptable risk of abuse. Under our State Constitution, in the absence of exigent circumstances, the installation and use of a GPS device to monitor an individual's whereabouts requires a warrant supported by probable cause.

[30] Loi n°78-17, relative à l'informatique, aux fichiers et aux libertés, 6 Jan. 1978.

[31] Markowitz, Kenneth J. "Legal Challenges and Market Rewards to the Use and Acceptance of Remote Sensing and Digital Information as Evidence." Proceedings of Duke Environmental Law & Policy Forum, Vol. 12 219, Spring 2002. 219-263.

[32] *Frye v. United States of America*, 293 F. 1013 (D.C. Cir. 1923).

[33] The relevance is determined according to FRE 402 and 403.

[34] Rychlak, Ronald J., Gabrynowicz Joanne Irene, Crowsey Rick. "Legal Certification of Digital Data: The Earth Resources Observation and Science Data Center

Among the strict limits within which the prosecutor has to establish the evidence of the facts, the respect of privacy certainly constitutes a major requirement.

Observing human activities using sophisticated technical devices, be they satellites or other optical or detection techniques might cause, at certain conditions, a violation of citizens' fundamental rights. The notion of 'search', as provided for by the IV Amendment of the U.S. Constitution, had to be clearly defined with regard to the new possibilities offered by technology to observe, most of the time from a very remote position, the details of someone's private life. Today, most of the national legislations provide for a dedicated set of rules applicable to the use of specific methods of investigation, including the conditions at which a warrant has to be issued by the judge prior to any observation.

Once again, the development by the U.S. jurisprudence of the notion of 'search' under U.S. constitutional law brings interesting considerations with regard to the acceptance by judicial bodies of new technologies' products. Two cases illustrate this development.

The *Ciraolo* Case[35]

The police had used an aircraft to take picture of a garden where cannabis plants were cultivated. The plantation was surrounded by flexible walls but not concealed by any roof, leaving the sight from above totally open. The Court of Appeal of California had rejected the pictures as admissible evidence ruling that such picture were the result of a search under the IV Amendment, thus requiring a warrant.

This decision was overruled by the Supreme Court considering that there couldn't have been any reasonable expectation of privacy since any people onboard an aircraft flying over the garden would have had the possibility to see the plantation. But this case was also the opportunity for the Court, in a dissenting opinion of Justice Powell[36], to assess the notion of 'privacy' with regard to the development of new means of observation:

> [A] standard that defines a Fourth Amendment 'search' by reference to whether police have physically invaded a "constitutionally protected area" provides no real protection against surveillance techniques made possible through technology. Technological advances have enabled police to see people's activities and associations, and to hear their conversations, without being in physical proximity. Moreover, the capability now exists for police to conduct intrusive surveillance without any physical penetration of the walls of homes or other structures that citizens may believe shelters their privacy.

The *Kyllo* Case[37]

In this apparently similar case fifteen years later, the police investigators had used a thermal sensor to observe individuals inside a house. Here, the words of Justice Powell sound quite relevant: the intrusive character of the thermal sensing allows observing activities and behaviours that would not be seen by any natural means, or by any persons not using the same device. Furthermore, this type of observation is particularly insidious to the extent that it reveals facts belonging to privacy and not supposed to be exposed to the general public. In this case, the Supreme Court ruled that the observation was a 'search' as under the IV Amendment, which required a warrant.

Transposed to satellite technologies, those two decisions seem quite relevant: satellites are indeed capable of detecting various activities and situations: some of them can be observed by natural means by any witness, others require the use of specific detection means (radar, thermal sensor, etc.). With the current resolution, it is obvious that satellites can be seen as a potential threat for privacy, especially considering that there is no means for the common people to be aware of the fact of the observation at any time.

Now, another question is the admissibility of a satellite observation revealing the fact of a criminal activity while the observation has been made for a totally different purpose. For instance, in the framework of a project of pollution monitoring of the land area, a set of satellite observations is realized on a portion of the territory with the purpose of enhancing spots where pollution by chemical substances is beyond the average level. While identifying those concentrations, scientists identify a portion of the territory corresponding to a private real property where chemical substances used for the production of synthetic drugs are abnormally present. Could the judge accept such observations as evidence of a crime? Would the answer be different if the police had directly ordered those observations?

Finally, two elements should also be taken into account when assessing the suitability of

Project." Journal of Space Law, Volume 33, nr 1, University of Mississippi, School of Law, 2007.

[35] *California v. Ciraolo*, 476 US 207 (1986).

[36] Ibid.

[37] *Kyllo v. United States*, 533 US 27 (2001).

satellite data for the purpose of establishing evidence at court.

The first one is the technical character of satellite observations. Contrary to aerial pictures, satellite data often need interpretation, notably through the use of dedicated software. Such an interpretation might require the intervention of an expert which constitutes an additional intermediary between the judge and the facts.

The second one is the availability of the data for all parties. It is true that with new multimedia services, access to satellite data has been considerably facilitated for the general public. Nevertheless, this concerns only a small part of the archives and doesn't apply to programmed observation which can be requested by authorities or companies. In the case of Hurricane Katrina disaster, it is not sure that all parties were on an equal foot when it comes to the actual access to the relevant data. Here again, the issue of certification surfaces: through a dedicated authority, both parties could have access to certified data which could be used at court in a contradictory procedure.

Apart from Contractual Law, Employment Law or Criminal Law, the use of satellite data in the framework of judicial procedures has also been illustrated by International Public Law. For instance, in several cases of border dispute settlements, the International Court of Justice has relied on the data provided by the satellite to solve the issue[38].

2.5.5 Conclusion

There might be a paradox in considering that the more accurate the satellite is, the more reliable it is but the more intrusive it becomes. Technical limits might be pushed further everyday, but the protective reaction is to legally limit this new capability.

The European Union INSPIRE Directive[39] illustrates the bargain between on the hand the willingness to take profit from technological upgrades (in constituting a global database with metadata at the European level) and on the other hand the need to protect the rights and interests of citizens. This explains the derogations to the principle of free access to geospatial data)[40].

The concept of *personal data* is certainly a key-concept in adapting to the new possibilities offered by the satellite. How could someone think, twenty-five years ago, that photographs taken from outer space could fall under the category of personal data? The protection of privacy is not so much about censorship, but rather about the control of the way information is used.

A coherent legal response must be applied to the technical chain of production of a satellite data, from the very moment it is acquired by the onboard instrument to the moment it is downloaded by an internet user. This is certainly not an easy challenge: from the State of registry which exercises control and jurisdiction on and onboard the satellite producing the data to the State where the derived products are used, a large variety of legal regimes is applicable. And it is only by working at the harmonisation of all those regimes that we may hope ending up with an effective and rational solution.

[38] *Burkina Faso v. Republic of Mali* of 22 Dec. 1986, CIJ and *Namibia v. Botswana* of 13 Dec. 1999, CIJ.

[39] Art. 13, Directive 2007/2/EC of the European Parliament and the European Council, establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) of 14 March 2007;OJ L 108

[40] Art. 13, Directive 2007/2/EC of the European Parliament and the European Council, establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) of 14 March 2007; OJ 2007 L 108.

3. Privacy Conflicts from High Resolution Imaging

3.1 Overview on Legal Issues

by George Cho

3.1.1 Introduction

This paper presents an overview of some of the legal issues pertaining to privacy in relation to high resolution imaging obtained from remote sensing platforms. The technology has given rise to conflicts and uncertainty in many spheres not least being those relating to the identification of individuals and raising privacy concerns. The legal implications of such conflicts and uncertainty can be severe and wide-ranging.

Experts in remote sensing by necessity are responsive and attentive to the rapid progress in technology. Legal practice and the law on the other hand are by design both reactive and slow to evolve. The half century of the so-called Space Age of space explorations has been accompanied by developments in international law and cooperation. This is evidenced by the five multilateral treaties and five resolutions and declarations that have been sponsored by the United Nations (UN) and more particularly the UN Committee on the Peaceful Uses of Outer Space (COPUOS). No other dimension of human activity has been so well shadowed by international cooperation and legal development (see Historical Background below).

3.1.2 Some Questions

In thinking about issues of privacy arising from the use of high resolution imaging, there are a number of fundamental questions that one might ask so that later discussions may be framed within such a context. The questions are:

- What is it that you want to keep private?
- Why do you want to keep it private?
- What are your rights to privacy?
- What are your responsibilities that go with such rights – to yourself, to your family and to society at large?

It is believed that answers to these questions might be fundamental building blocks for tackling the questions of privacy in general and more specifically the conflicts that may arise from using high resolution satellite images. The feeling that technology may have eroded our personal privacy is a real one. But here there is a need to try and strike a balance between what is private to an individual as against what is in the public arena and to be shared by all. Privacy violations both advertent and inadvertent are difficult to protect and to police.

In this paper it is proposed to look at four aspects of the privacy question and then to propose a framework for addressing privacy conflicts. However, before addressing these issues there is a preliminary matter of outlining the historical background to space law and to sketch the present legal framework. From that background it could be surmised that the privacy question is but yet just another spoke to the umbrella of legal issues. The first aspect of the privacy question is to consider privacy as a legal matter. This is followed by a second section that summarizes the legal framework and outlines the various legal theories that may be used to discover infringements of privacy rights and relevant remedies. The third section addresses privacy concerns emanating from the use of high resolution remotely sensed images.

3.1.3 Historical Background to Space Law

As intimated in the preliminary paragraphs there are to date five multilateral treaties and further five declarations and resolutions. Most of these treaties and declarations come within the purview of the UN Committee on the Peaceful Uses of Outer Space (COPUOS). The main themes of each of these in chronological order may be paraphrased as follows:

Treaties

1966 Treaty governing activities of states in the exploration and use of Outer Space

1967 Agreement on the rescue of astronauts

1971 Convention on international liability for damage caused by space objects

1974 Convention on registration of objects launched into Outer Space

1979 Agreement governing activities of states on the Moon and other celestial bodies

Declarations

1962 Declaration of legal principles governing activities of states in exploration and use of Outer Space

1982 Principles governing use by states of artificial Earth satellites for TV broadcasting

1986 Principles relating to remote sensing of Earth from Outer Space

1992 Principles relevant to the use of nuclear power sources in Outer Space

1996 Declaration on international cooperation in exploration and use of Outer Space

Professor Frans von der Dunk has published two very important papers in regards to space law. The first is his seminal paper on 'Sovereignty versus space – Public law and private launch in the Asian context' published in 2001.[41] In the paper he observed that there has been an almost complete silence in international space law on private entities and private activities. The absence of attention on private enterprises may be because space law was conceived as public international law and that states were the only legal personae at that time undertaking space exploration. It also may be because at the start of the Space Age there were no private 'players' on the scene given that space exploration was by and large an activity funded by the state. Perhaps only in the last decade has there been privately funded space activity mainly in telecommunications. That paper also raised important issues of territorial jurisdiction and space activities, space law responsibility and state liability and several looming practical problems.

The second important paper that Professor von der Dunk published was on 'The Legal Aspects of Geospatial Data Gathering in Space' (2005). [42] In this paper he noted the lack of focus on legal regulation. The paper is more critical of recent developments because the international legal environment was fragmentary where the extant rules and principles at the international level were often ill-defined and open to legal interpretation. The regulations have been confined to certain territories, to certain forms of activities and to certain types of natural or legal persons. In some others, there have been no specific application rules or principles.

Professor von der Dunk (2005) concedes that the 1967 Outer Space Treaty does provide a basic legal framework for all activities in space from the freedom of exploration, the principle of non-appropriation by any single state of Outer Space to the application of general international law to Outer Space in terms of the gathering information freely. More importantly the 1986 UN Resolution 41/65 outlined the legal principles pertinent to remote sensing. While not a precise legal document, the Resolution has been adopted by consensus and has become part of international customary law and hence is binding on states. Of the dozen or so principles the one that is presently most relevant relates to Principle XII that provides a right of access by sensed State to data concerning its territory on a 'non-discriminatory' basis. This is in addition to the absence of rights to preclude its territory from being sensed nor any right to an exclusive and priority access to such data.

Resolution 41/65 provides very general guidelines in regards to intellectual property rights (IPR) to the data and the potential liability and compensation where such data were erroneously used and interpreted; and the potential value of the data as evidence in a court of law. In practical terms, there is uncertainty as to the application of these guidelines at an international level. Also there are issues of liability where there may be intergovernmental partnerships and transnational and private entities involved. In the case of liability, Professor von der Dunk points to partial solutions embedded in the 1972 Liability Convention and the 1975 Registration Convention. But these still require the need to promulgate national legislation to implement domestic law to control and monitor private activities in space. The Resolution does not directly address issues of privacy or data misuse at the level of the person. There is yet more work to be done before the legal environment becomes more certain.

Professor Ito (2008) echoes similar observations when she laments an urgent need for clarification in the use of geospatial data and a more comprehensive legal regime.[43] In her paper Ito examines the current legal framework, the shortcomings of the current regime and the associated legal issues and proposes

[41] von der Dunk, F. "Sovereignty versus space : public law and private launch in the Asian Context". Singapore Journal of International and Comparative Law 5 (2001): 22-47.
[42] von der Dunk, F. "Legal aspects of geospatial data gathering in space." GIM, International. Vol. 19 8 (2005): 69-71.
[43] Ito, A. "Improvement to the Legal Regime for the Effective use of Satellite Remote Sensing Data for Disaster Management and Protection of the Environment". Journal of Space Law. Vol. 34 (2008): 45 – 65.

improvements to the system. The inadequacies of the existing regime include divergent data policies among states, the ambiguity over responsibility and liability arising from suppliers and/or the misuse of the data, restrictive access and pricing policies and third party risks and damages arising from the use of incorrect data. Further uncertainty is engendered where IPR are undefined and other liability risks from the use of the data are unidentified. In discussing the above issues, Professor Ito also refers to the *Disaster Charter* (2000) where signatories assist each other and other states in the event of natural or technological disasters.[44] Such an organic development demonstrates the felt need among signatories and necessity for a cooperative agreement in times of crisis. Professor Ito offers several suggestions to address issues of data policies and liability and how disputes may be resolved either under contract or tort liability. The plea from this paper is the increasingly important role that the legal framework could play if remotely sensed data are to be exploited to its ultimate capabilities.

In the brief survey of the literature above one may note the legal issues identified include: issues of liability and damage, the regulation of private entities, international regulation embedded as national customary law, IPR and jurisdiction. Together these issues either singly or in concert can be complex and difficult to resolve without some international regulation and without an overarching legal framework. Indeed the Third UN Conference on the Exploration and Peaceful Uses of Outer Space (UNISPACE III) held in Vienna in July 1999 identified some challenges to space law. These challenges include space launch services, space traffic, tort liability in regards to financing and insurance, IPR and other emerging legal issues such as space debris, unforeseen activities and the space environment. Among these one unforeseen activity is the rapid development of global positioning system (GPS) technology that has blossomed to become a leading instrument that perversely creates potential privacy issues. Professor Jasentuliyana (2001) asks the question as to whether there is a public international space law framework that can cope with these new developments and the need for "more clarification and precision for addressing an extremely sophisticated and diverse space industry" – one which is also privatised and commercially intense.[45]

The issue of privacy, as is presently understood, has only recently surfaced to command the attention of regulators and the international citizenry. It seems that it is now timely that the topic of privacy and all its implications should be fully debated and some framework for its regulation devised. Privacy may seem to be the 'final frontier' given its intense gaze with the use of high resolution remotely sensed imagery that when combined with other data give rise to powerful tools that may be employed for good and for evil.

3.1.4 Privacy as a Legal Matter

Privacy is a fundamental human right and is the very basis of human dignity and values. Privacy also ensures that there is a freedom of association and freedom of speech. Such a right is protected by the Universal Declaration of Human Rights (UDHR) adopted in 1948 and the International Covenant on Civil and Political Rights (ICCPR) 1976.[46] Nearly every country has a right of privacy in its Constitution with protections against intrusions of one's home, the confidentiality of communications and specific rights to access and control of one's personal information. Where such rights are not provided for in the Constitution, courts have found other means of giving protection. The same words are found in the Declaration and Covenant as follows:

> » No one shall be subject to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attack.[47]

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950 (ECHR) is in a similar form. Article 8 guarantees a right to respect of a person's private and family life, home and correspondence and that no public authority has the right to interfere with this right except in accordance with the law and as necessary in a democratic society in the interests

[44] Art. 3.1, "Charter on Cooperation to Achieve the Coordinated Use of Space Facilities in The Event Of Natural or Technological Disasters." Rev. 3 (25/4/2000). 24 June 2010. <http://www.disasterscharter.org/web/charter/charter>.

[45] Jasentuliyana, N. "International Space Law Challenges in the Twenty-first Century." Singapore Journal of International and Comparative Law, 5 (2001):10-21.

[46] Art. 12, Universal Declaration of Human Rights, Paris, UN GA Res. 217 A (III) of 10 December 1948. A/RES/217; Art. 17 International Covenant on Civil and Political Rights, New York, done 19 December 1966, entered into force 23 March 1976.

[47] Ibid.

of national security, public safety or economic well-being of the country.[48]

Delving back in history there are also deep roots to the recognition of a right to privacy in the Qur'an to the sayings of Mohammad, to references in the Bible and to Jewish law.[49] However, there is no universal definition for privacy and varies according to the context and usage. The concept of privacy may also differ between cultures and legal traditions. At times privacy is also fused with the management of personal information. Hence, the protection of one's privacy is seen as a means of delineating the permissible degree of intrusion to a person's life and the rights of a person to be left alone.

To reiterate, privacy has emerged as a topic demanding attention and this no more so than in the application of geospatial technologies. *Slonecker et al.* (1998) believe that the combined effects of new generation high resolution imagery, the privatisation of the remote sensing industry and the development of the global information infrastructure (GII) have inadvertently conspired to produce significant legal and ethical consequences for the remote sensing community.[50] The detail, resolution and scale of modern remote sensing bring into sharp focus the various issues of personal privacy.[51] There may be advertent or inadvertent violations of privacy in some applications. Technological developments have gone hand in glove with others such as facial recognition, biometrics, the digital revolution and powerful sensor devices that may seem to exhaust all rights to privacy of the individual. Ironically, some of these may be officially sanctioned as in the case of closed-circuit television (CCTV) in Britain. CCTV poses both ethical and legal questions and may be the price one pay's for living in a digital age where a snail trail of data is left behind everywhere we go.

Given these erosions to privacy, there are some who believe that governments have a civic responsibility to their citizens to ensure that the infrastructure that they deploy contain privacy protections (Blumberg & Eckersley 2009).[52] However, Westin (1967) in the alternate has suggested that the 'invisible economic hand' would ensure that information technology (IT) did not result in excessive privacy invasion and therefore any form of privacy regulation was unnecessary. To the extent that any regulation was imposed, it was important that there were minimal impacts on business and government activities.[53] But as will be observed from the discussion to follow, there is a need to regulate such activities precisely to protect privacy interests.

In terms of the concept of privacy, tidy minds might wish a strict dividing line between what is private and what is public, but in reality there seems to be a continuum of sorts. This 'continuum' delineates those parts of our lives that relate to personal information about ourselves, our financial status, health, and education. At times some of the personal information about us may meld into what might be considered in the public domain where there may be no privacy.

Professor Arthur Miller of the Beckman Center for Internet and Society, Harvard Law School has described privacy as an intensely, perhaps, uniquely, personal value. The word 'privacy' stems from a Latin root *privare* which means 'to separate'. To want privacy is to want to be separate, to be an individual. *Privare* also means to deprive, to take, to rob or to leave something behind.[54] So as individuals we may have interests to sustain our 'personal space' free from interference by other people and organisations.[55]

One way of conceptualising privacy is to consider its multidimensionality. A typology to describe the various facets of the concept seemingly falls into four interlocking themes.[56]

[48] Convention for the Protection of Human Rights and Fundamental Freedoms, (ETS No. 005), entered into force 3 September 1950. Rome, 4.XI.1950. Council of Europe.

[49] an-Noor 24:27-28 (Yusufali); al-Hujraat 49:11-12 (Yusufali) for Koranic references; Volume 1 Book 10 Number 509 (Sahih Bukhari); Book 20 Number 4727 (Sahih Muslim); Book 31, Number 4003 (Sunan Abu Dawud) for the sayings of Mumammad; Hixson, RF (1987) Privacy in a Public Society: Human Rights in Conflict (New York: Oxford University Press) for biblical references and Rosen, J (2000) The Unwanted Gaze (New York: Random House) for references to Jewish law.

[50] Slonecker, E.M., Shaw, D.M. and Lillesand, T.M. "Emerging Legal and Ethical Issues in Advanced Remote Sensing Technology." Photogrammetry Engineering and Remote Sensing. Vol. 64 no. 6 (1998): 589-595.

[51] Space Imaging now GeoEye's new generation high-resolution satellite the IKONOS launched in September 1999 can detect objects of 1 m in size anywhere on Earth and has a data collecting rate of about 2,000 square kilometres per minute. 24 June 2010 <http://www.geoeye.com/>

[52] Blumberg, A and Eckersley, P. "On Locational Privacy and Hot to Avoid Losing it Forever." Electronic Frontier Foundation 24 June 2010 <http://www.eff.org/files/eff-locational-privacy.pdf>

[53] Westin, AF. "Privacy and Freedom." New York: Atheneum, 1967.

[54] Beckman Center for Internet and Society. "Privacy in Cyberspace." 24 June 2010 <http://eon.law.harvard.edu/privacy99/syllabus.html>.

[55] Clarke, R. "What is Privacy?" Xamax Consultancy PL Australia. 2006. 24 June 2010 <http://www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html>.

[56] Clarke, R. "Privacy Impact Assessment in Australian Contexts." E-Law Journal 15 (2008). 24 June 2010 <https://elaw.murdoch.edu.au/archives/issues/2008/elaw_15_1_Clarke.pdf>.

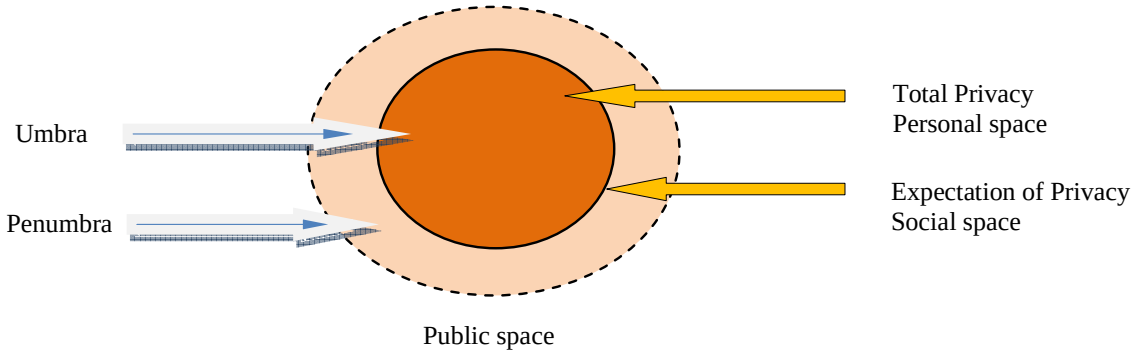


Figure 3.1: Zones of Privacy: Umbra and Penumbra

- *Bodily privacy* which relates to the protection of a person against invasive procedures such as genetic tests, drug tests and body searches as well as other forms of covert checking of the person.
- *Information privacy* also known as data protection relates to the rules governing the collection and handling of personal data such as medical and Government records, financial records.
- *Privacy of communication* that gives security and privacy of mail, telephones, electronic mail and other forms of communication.
- *Locational privacy* sets limits on intrusion into domestic and other places such as at work or in public spaces – this includes searches, video surveillance and identity checks as well as one's geographical location and position in space.

This typology may be summarised as: who we are, what we know, what we say and where we are.

The typology above suggests a continuum of privacy interests, of 'zones' of privacy, and of personal, private and public space.[57] It may further suggest that such 'spaces' may be thought of as both 'vertical' and 'horizontal'. The continuum of what is in the private domain and what is in the public domain may be visualised as being laid out horizontally in a linear fashion that portray varying degrees of privacy. The boundary demarcating one from the other is 'fuzzy' at best given that there may be various parameters that are at play from the totally selfish one to the totally selfless one – in the public interest. The width and placement of the demarcation line could be weighted in terms of political interests, economic interests as well as other interests including religious and cultural ones. From such a conceptualisation we may have a core part that gives total privacy to a person – the *umbra* (similar to the dark central part of a sunspot). Then there is the *penumbra* – the partially shaded region around the umbra (of the person) where there may be lesser degrees of privacy. Finally, outside these two areas is the public area where there may be no privacy at all.[58]

But note also that personal 'spaces' may be culturally defined. In some cultures there can be very close contact between and within genders in public whilst in other cultures it might be taboo to be either seen holding hands or simply seeing the face of the person. The linear-continuum treatment of the privacy question can also have a third dimension in the vertical space above. In the English common law tradition much use has been made of the Latin maxim *cujus est solum ejus est usque ad coelum et ad inferos* (he who owns the surface of land also owns the sky stretching to the limits of the atmosphere and all the soil to the centre of the earth).[59]

Applying this idea by analogy to the privacy of a person, it is suggested that a person may have a right to privacy in the 'space' above. Any intrusion of this space – the vertical zone – is an intrusion of privacy. Some may consider this suggestion to be absurd and fanciful and totally inapplicable under the

"Overview of Privacy." Privacy overview 2007. 24 June 2010 <http://www.privacyinternational.org/article-shtml?cmd[347]=x-347-559062>.

[57] In 1965, the U.S. Supreme Court suggested that there may be 'zones of privacy' implicit in the Bill of Rights in the leading case of *Griswold v. Connecticut* (1965) 381 U.S. 479; 14 L.Ed.2d 510; 85 S.Ct. 1678.

[58] The penumbra argument has been put previously by Scoglio, S. "Transforming Privacy: A Transpersonal Philosophy of Rights.", Westport: Praeger, 1998: 226.

[59] Coined by Accursius in Bologna in the 13th C. See cases on ownership of airspace in Re Lehrer and the Real Property Act [1960] NSWR 570; (1960) 61 SR (NSW) 365 Supreme Court of NSW in Equity; *Kelsen v Imperial Tobacco Co* (of Great Britain and Ireland) Ltd [1957] 2 QB 334; [1957] 2 All ER 343; [1957] 2 WLR 1007 English High Court of Justice, QB Division; and *Bernstein of Leigh (Baron) v Skyviews and General Ltd* [1978] 1 QB 479 QB Division.

circumstances. But, be that as it may, the central theme is to try to view the privacy question in all its facets so that the informational privacy including relationships, property ownership, temporal and other activities of an individual is coupled with the spatial aspects of privacy. The idea is even more apposite when dealing with remotely sensed images that include the possible identification of persons on the ground. It is an important question because of what society constitutes to be basic personal privacy and what is regarded as potential invasions to privacy. This is no more so because of the difficulties in grappling with the very concept of privacy.

Another idea that may have currency in this discussion of privacy is the saying that one man's home is his castle. This idea has been encapsulated in the English Common Law tradition of protecting the home against government intrusion.[60] This principle has developed to take the form of the U.S. legal doctrine known as 'Castle law' or 'Defense of Habitation law' that designates one's place of residence as a place in which one enjoys protection from illegal trespassing and violent attack and this includes the *curtilage* – the enclosed area of land around a dwelling. Both the home and the *curtilage* provide a reasonable expectation of privacy.[61]

Common Law Privacy Rights and Protections

In the common law world the claim to privacy as a right is a relatively recent phenomenon because of the *ad hoc* nature of the protection of privacy in the past. The Australian Constitution, for example, has no vested powers over privacy protection while the common law protects privacy rights indirectly. For example, the law of defamation, negligence, and passing off give a semblance of protection of privacy as do contract law and the duty of confidence. However, the Australian Parliament has been obligated to protect personal privacy stemming from various international covenants, agreements and treaties to which Australia is a signatory, for example, UDHR and ICCPR.

Since the majority decision in *Victoria Park*[62] it has generally been accepted that a cause of action for the breach of privacy does not exist in the common law of Australia any more than it existed in the common law of England.[63] The issue of a right to privacy was revisited in Australia recently in a High Court case.[64] In the U.K. the right of privacy of a corporation has been held to exist.[65] Also more recently privacy rights have also been extended to individuals drawn from the fundamental value of personal autonomy.[66] Courts in several other jurisdictions have also addressed the availability under common law of an actionable wrong of invasion of privacy – Canada, India, and New Zealand.[67] One Canadian court has recognised a general right to privacy and to protect privacy interests under the rubric of nuisance law.[68] In New Zealand the tort of invasion of privacy has been recognised in s 14 of the *New Zealand Bill of Rights Act* 1990 (NZ) but while it does not confer a right to privacy it ensures the freedom of expression (Tobin 2000).[69]

In the U.S. the origins of the privacy right may be traced to a law review article by Warren and Brandeis (1890).[70] In a famous dissenting opinion, Judge Louis Brandeis in 1928 reiterated the right to be left alone as "the most comprehensive of rights and the right most cherished by civilised men".[71] Based on the principle of the right to be left alone, U.S. law has developed along the lines of a common law right and those rights found under the various Amendments to the U.S. Constitution. A right to privacy is absent in the U.S. Constitution and is not found in the Bill of Rights. However, the U.S. Supreme Court has interpreted a right to individual privacy under the First, Fourth, Fifth, Ninth, and Fourteenth Amendments. Many privacy decisions in the U.S. federal courts are based on the Fourth Amendment, which generally provides for the right of people to be secure in their persons,

[60] William Pitt's address in 1763 to the House of Commons where he said "The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain may enter – but the King of England cannot enter – all his force dares not cross the threshold of the ruined tenement". Speech on Exercise Bill, 1763.

[61] The term "Make my day law" has been used to describe this law and comes from the landmark 1985 Colorado statute that protects people from any criminal charge or civil suit if they use force – including deadly force – against an invader of the home. The law's nickname is a reference to the famous words uttered by Clint Eastwood's character Harry Callahan in the 1983 film Sudden Impact … "go ahead, make my day".

[62] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* [1937] 58 CLR 479; 43 ALR 597 (HCA).

[63] *R v Khan* [1997] AC 558 at p. 582-3.

[64] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63, 15 November, 2001.

[65] *R v Broadcasting Standards Commission*; ex parte British Broadcasting Corporation; (2000) 3 WLR 1327; (2000)3 All ER 989.

[66] *Douglas v Hello! Ltd* [2001] 2 WLR 992; (2001) 2 All ER 289 per Sedley LJ: 120.

[67] *Aubrey v …ditions Vice-Versa Inc*. [1998] 1 SCR 591; *Govind v State of Madhya Pradesh* [1975] 62 AIR (SC) 1378; P v D [2000] 2 NZLR 591.

[68] Canadian Tort Law, 6th ed. [1997] at 56; *Aubry v Duclos* [1996] 41 DLR (4th) 683.

[69] Tobin "Invasion of privacy". New Zealand Law Journal 216 (2000).

[70] Warren, S., Brandeis, L. "The Right to Privacy." Harvard Law Review 4 (1890):193.

[71] *Olmstead v. U.S.* [1928] 277 U.S. 438.

houses, papers, and effects against unreasonable searches and seizures.

3.1.5 Legal Frameworks and Legal Theories

3.1.5.1 Legal Frameworks

There are possibly four different legal frameworks that have been devised for privacy protection in various parts of the world. Some frameworks are prescriptive whilst others are options to be exercised by individuals. Because there is a spectrum for these, the frameworks can be complementary and contradictory. In practice the use of all four within the same jurisdiction can be effective.

1. Comprehensive laws. The E.U., for example, uses a data protection regime in the form of a Directive, whereas elsewhere in Australia, New Zealand and Canada a co-regulatory model is used. In the latter cases the laws are developed by industry groups but overseen by a public officer or agency. Such laws are presumptive of powers that enable legislation on the subject matter.
2. Sectoral laws. This is the hallmark of privacy protection laws in the US and stems from its federal and state structure with certain sectors of the economy being governed federally. Hence there are legislation protecting the privacy of communications – electronic or otherwise, credit reporting, debt collection, financial, protection of children, driver licences, video rentals, health insurance, education rights and one's location. There may be parallel state legislation which sometimes might run counter to the intent at the federal level and vice versa. The major drawback with this model is that there is a need to promulgate new laws when mass use new technologies emerge. It is possibly here that there is a 'lag' in that technological developments might gallop ahead of the law which has not kept pace. Also there may be the need for an oversight Agency to ensure consistency, compatibility and currency with such laws and to provide the strategic vision. In some countries such sectoral laws are used in conjunction with the comprehensive laws.
3. Self-regulation. Self-regulation is another means for the protection of privacy and comes in the form of a national privacy principles, 'soft-touch' code of practice, self-policing and industry standards. These codes are developed by industry as well as the clients who use the technology.[72]
4. Technologies of privacy. Clarke (1999) has identified three types of technologies.[73] First, there are privacy-invasive technologies (PIT) including 'data-trail generation through the denial of anonymity, data-trail intensification as in identified phones, stored value cards (SVCs), intelligent transport systems (ITS), data warehousing and data mining, stored biometrics, and imposed biometrics'. Second, there are privacy-enhancing technologies (PET) that have been developed in the last decade as a reaction to and as an attempt to reverse trends identified in PIT above. Examples include the Electronic Privacy Information Centre's (EPIC) list of enhancing-tools where privacy practices may be retrieved by user agents (or 'bots' – robots).[74] Third, privacy-sympathetic tools (PST) deliver genuine anonymity such as various pseudo-identifiers and digital persona together with pure data protection.

The voluntary standards and codes of practice may work well in Australasia, Canada and the U.S. while civil law countries like in the E.U. appear to favour legislation and mandatory standards. Whatever framework is used the message is that the laws and regulations specifying how privacy protection is to be achieved must be clear, consistent and technology-neutral.

3.1.5.2 Legal Theories

In seeking to apply legal theory to the analysis of the protection of privacy it may be relevant to suggest that in the main that there are two traditions of law that are extant around the world – the common law based on the English legal tradition and civil law of the Roman and Continental tradition. However, it may be said that whether it is by precedent or by codified law, the legal theories used are similar. Here while the focus is on the legal issues that are brought up by geospatial technologies an in-depth discussion on the technicalities of the law is avoided.

[72] E.g. the Australian National Privacy Principles for Handling Personal Data promulgated in the Privacy Act 1988 (Cwlth) Schedule 3.
[73] Clarke, R. "The legal context of privacy-enhancing and privacy-sympathetic technologies", 1999. 24 June 2010 <http://www.anu.edu.au/people.Roger.Clarke/DV/Florham.html>
[74] EPIC Online Guide to Practical Privacy Tools (2003). 24 June 2010 <http://www.epic.org/privacy/tools.html>.

From this writer's viewpoint there appear to be four major legal theories that will be touched upon by geospatial technology and these are property law, confidentiality, environmental law and tort liability and nuisance. Property law is included because geospatial technologies in the form of satellite imagery will capture any geographical space on Earth. Confidentiality of communication is included from the point of view of data protection especially as it relates to information about a person, the reputation of that person and the protection of privacy generally as a result of data integration with high resolution imagery. Environmental law is another theory that is included especially in regard to ownership of the airspace above the land parcel. Finally, tort specifically in terms of liability, damage and personal injury arising from integrating data with high resolution imagery is pertinent to this discussion.

The proposal here is to investigate each of these theories separately and provide case materials where relevant from litigation reported from selected jurisdictions. Examples are drawn from the U.S. Canada, U.K., Australia, New Zealand and the common law world generally. These examples will provide the facts of the case and the legal principle at issue. The major challenge is that of the protection of privacy and while there is little legal guidance with geospatial data, there is a lot of legal precedence with other types of personal data. The lessons from similar cases and legal applications may be salutary.

Trespass to Land – Property Law

Reference is made to an earlier reference to the Latin maxim *cujus est solum ejus est usque ad coelum et ad inferos*. The ownership of land is said to give proprietary rights to the airspace above the land and the earth below. However, these two 'rights' have now been circumscribed given that the airspace far above the practical space has been surrendered for public use of airplanes and other vehicles.[75] Similarly the space below the useable land, where it contains mineral wealth, is 'owned' by the Crown as of right. In regard to real property ownership, the two causes of action that may lie are either in terms of trespass of the land or nuisance. The question that arises is whether there is any trespass of the land when a satellite circling above the land is taking high resolution imagery.

Trespass is a wrong or tort where a trespasser 'broke the close' or entered the land of another without lawful authority. So, what is the position of imagery taken of the land by remote sensing satellites? The imaging does not need any form of physical incursion onto the land or territory owned by the person.

There has been some U.S. litigation involving geospatial technologies on the basis of 'trespass' to land. The grounds on which these cases have been argued include either the idea of an 'objective' expectation to privacy found in the Fourth Amendment to the U.S. Constitution or a 'subjective' expectation as provided under case law interpretations as the following cases demonstrate.[76]

In *Dow Chemical v United States* (1986) at first instance a District Court held that the aerial photography was a "violation of Dow's reasonable expectation of privacy and an unreasonable search in violation of the Fourth Amendment".[77] On appeal, the U.S. Supreme Court held that the "open field" doctrine applied to the case, and therefore there was no invasion of privacy – the open field as a term of art referring to the public spaces around the Dow property.

Similarly in *California v Ciraolo*[78] the Supreme Court found that it was acceptable for the police to fly over a fenced-in backyard at an altitude of 1,000 feet (305 m) to undertake monitoring. Also in *Florida v Riley*[79] a court approved the use of a helicopter, hovering at 400 feet(122 m), to observe marijuana plants through a hole in the roof of a defendant's greenhouse.

The remit to observe from the air has also extended to monitoring emissions. In *United States v Penny-Feeny*[80] a Hawaii District Court endorsed the police use in a helicopter of a forward looking infrared (FLIR) device to discern heat emissions from a garage to gather information on illegal activities. Beepers and identity tags have also been endorsed to track the location of individuals in

[75] "… restricting the rights of an owner in the airspace above his land to such height as is necessary for the ordinary use and enjoyment of his land … above that height he has no greater rights in the airspace than any other member of the public" per Griffith, J. *Bernstein of Leigh (Baron) v Skyviews and General Ltd* [1978] 1 QB 479.

[76] The Fourth Amendment of the U.S. Constitution, guarantees freedom from unreasonable search and seizure, including (in some cases) electronic, aural, visual and other types of surveillance.

[77] *Dow Chemical v United States*(1986) 106 S.Ct. 1819, 90 Led 2d 226.

[78] *California v Ciraolo* (1986) 106 S.Ct. 1809; (1986) 476 U.S. 207.

[79] *Florida v Riley* (1988) 488 U.S. 445.

[80] *United States v Penny-Feeny* v 773 F.Supp. 220 (D. Haw. 1991).

motor vehicles and then use GIS to map and trace routes.[81]

In *United States v Smith*[82] a U.S. Court of Appeals for the Fifth Circuit has ruled that technological advances may be capable of expanding the legally protected range of privacy that individuals enjoy. In *United States v Causby*[83] the U.S. Supreme Court held that continued low-altitude flights by military aircraft which ruined the plaintiff's poultry business constituted a wrongful 'taking' of private property and under the Fifth Amendment required compensation.

U.S. property law has been described as both exceptionally simple and exceptionally rigorous and makes distinctions between the person and the property.[84] Of particular interest is the vertical extent of the property. Any physical entry upon the surface of the land without permission is a trespass, whether it be by walking upon it, flooding it with water, casting objects upon it, or otherwise. One may commit a trespass upon the vertical surface of another's premises, as well as the horizontal. There is thus a property right in the airspace above land, which may be invaded by overhanging structures or telephone wires, by thrusting an arm across the boundary line, or by shooting across the land, even though the bullets do not fall upon it.

Four distinct legal theories of trespass have been evolved to help analyse the conflicting interests of the surface owner and the aviator.

- One is the 'zone' theory which divides the airspace into two strata, with the landowner owning that contained in the lower zone, but not that in the upper. The line is drawn at the limit of the owner's 'effective possession', or in other words, at so much of the space above him as is essential to complete use and enjoyment of his land. The height of the zone of ownership must vary according to the facts of each case. This rule was applied in *Smith v New England Aircraft Co*.[85] where flights at the level of 100 feet (31 m) were held to be trespasses, since the land was used for the cultivation of trees which reached that height.
- A second view is where a court refused to find a trespass in flights even within 5 feet (1.5 m) of the surface of unoccupied waste land. The decision denies any ownership of the unused airspace, and limits the owner's rights to his actual use of it. The rule that has evolved is that there is no tort unless there is interference with the present enjoyment of the property.[86]
- Restatement of Torts §194 has been taken over by the Uniform State Law for Aeronautics and enacted in one form or another in some 22 states. This section recognizes unlimited ownership of upward space, subject to a privilege of flight similar to the public right to make use of a navigable stream – a view now possibly discredited with the advent of space voyages.
- Finally 'nuisance theory' ignores arguments about ownership of the air and gives a remedy in the form of an action for nuisance or negligence. Such a remedy is available where the flight results in actual interference with the use of the land and is unavailable without such interference.[87]

In a further case where trespass, nuisance and privacy have come together is that of the California Coastal Records Project. This project maintains a website that provides an aerial photographic survey of the California coast for scientific and other researchers. The entire California coastline has been photographed from a small helicopter—one picture every 500 feet (152 m)—from the Golden Gate Bridge to the Hearst Castle. The objective of the project is to provide a baseline for conservation and other land use researchers.

The Hollywood actress Barbara Streisand sued the photographer and two other defendants for US$10 million in May 2003, claiming that the pictures they provided to others of her Malibu home and estate violated her right to privacy and violated the California's Anti-Paparazzi Act. A Los Angeles Superior Court decision in December reaffirmed the public's First Amendment right to participate in matters of public significance as well as the freedom of expression. In addition the court rejected her claims to privacy and violations of the Anti-Paparazzi Act and further held that Ms Streisand had abused the judicial process by filing the lawsuit. The court also rejected her request for an injunction to remove the panoramic photographic frame of

[81] *United States v Knotts* (1983) 460 U.S. 276 *United States v Karo* (1984) 468 U.S. 705.
[82] *United States v Smith* (1992) No. 91-5077 5th Cir. Nov, 12.
[83] *United States v Causby*(1946) 328 U.S. 256.
[84] Prosser, WL. 1971 "Handbook of the Law of Torts" (4th edition). St. Paul. West Publishing Co.: 63.
[85] *Hinman v Pacific Air Transport* (1930) 270 Mass. 511, 170 N.E. 385.
[86] *Hinman v Pacific Air Transport* (1936) 9th Cir.; 84 F.2d 755, cert. denied 300 U.S. 654.
[87] *Delta Air Corp. v Kersey* (1942) 193 Ga. 862; 20 S.E.2d 245.

her bluff-top home and property from the Coastal Records Project.[88]

These cases demonstrate attempts to balance the rights of property interests of the land-owner and the demands of the growing geo-spatial industry that has become highly important to the public. While some of the distinctions can be highly artificial, a majority of the decisions rest upon the key ingredient of an unreasonable interference and particular facts.[89]

Confidentiality and Data Protection

A legal duty of confidentiality may arise in equity, at common law or under contract. In the main we are dealing with confidential information that may not be disclosed to a third party without consent. Normally trade secrets are in this genre and the parties may be in a contractual relationship. However, at times there may be information of a sensitive nature that may need protection. Sensitive personal information includes health matters, political beliefs, religious affiliation, sexual preferences, membership of political parties and the like. In the case of geospatial information one may ask whether the image of one's home is considered personal information. If it is not, then there are no privacy issues arising from it. If it is personal information then there are privacy implications because at a minimum people need to know what other people know about them.

An example is the following case of *Naomi Campbell v Daily Mirror*.[90] Here *The Daily Mirror* newspaper published a photograph of the supermodel's attendance at a narcotics support group. Ms Campbell sued for breach of confidence. *Morland J.* at first instance in the High Court ruled in favour of the supermodel. On appeal, the Court of Appeal found that the disclosure was not in breach of an obligation of confidentiality. The Appeal Court found that Ms Campbell's Art. 8 rights under the UK's *Human Rights Act* 1998 were overridden by the newspaper's Art. 10 right, since disclosure of her drug abuse problem was in the public interest. However, the House of Lords overturned the Court of Appeal judgement by 3:2 and ruled that the *Daily Mirror* had violated Ms Campbell's right to privacy. *Lord hope of Craighead* said that '[d]espite the weight that must be given to the right to the freedom of expression that the Press needs if it is to play its role effectively, I would hold that there was here an infringement of Miss Campbell's right to privacy that cannot be justified'.

But the above case may be contrasted to that of *Douglas v Hello! Ltd.*[91] In April 2003 the High Court decided that there was no free-standing right to privacy in the U.K. The well-known actors Catherine Zeta-Jones and Michael Douglas had sued *Hello Magazine* for the unauthorised publication of their wedding photographs. The court held that the law of confidence was sufficient to protect people in Douglas's position. The court used the analogy of people who traded on their image rights with that of manufacturers trying to protect confidential trade secrets.

In the U.K. the law is uncertain as to when confidentiality is breached and when rights to privacy may be asserted. The uncertainty is because of particular fact situations so that in the *Campbell* case it was at a specific location whereas in the *Douglas* case it was a matter of a contractual relationship because the actors had long-standing arrangements with another magazine publisher.

The legal protection of privacy can also be made using trespass, defamation and racial vilification laws. Legislation in Australia offers protection from surveillance of any kind. For example, it is impermissible to undertake surveillance or interfere with one's home or family, or uncover sensitive facts relating to an individual's private life. While technology today ensures that we have become less able to do things invisibly one must be mindful of the opposite case of *sousveillance* – covert or otherwise – also described as the inverse of surveillance. *Sousveillance* is 'watchful vigilance from underneath' and is possibly derived from the French *sous* – meaning below as opposed to *sur* – from above. This method has been used in the Cambridge MESSAGE Study in 2008 where data collectors were sent out to gather air pollution data on mobile devices which tracked their every movement and location.[92]

Some jurisdictions have resorted to full-scale legislation that is harmonised and implemented across all states. An example is the E.U. Data Directive entitled *The Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data* that became

[88] *Streisand v Adelman Case* No. SC 077 257 Cal. W.D. 31 December 2003. 24 June 2010 <http://www.californiacoastline.org/streisand/slapp-ruling.pdf>

[89] Prosser, WL 1971 "Handbook of the Law of Torts" (4th edition), St. Paul, Minn: West Publishing Co.

[90] *Campbell v Mirror Group Newspapers* [2002] All ER (D) 448 (March); [2003] QB 633.
See also, *Campbell v Mirror Group Newspapers* [2002] All ER (D) 177 (October). 24 June 2010 <http://www.lawreports.co.uk/qbmarb0.3.htm>.

[91] *Douglas v Hello! Ltd* [2003] All ER (D) 209 (April).

[92] "Cyclists' cellphones help monitor air pollution." 24 June 2010 <http://technology.newscientist.com/article/dn13130-cyclists-cellphones-help-monitor-air-pollution.html>.

effective on 25 October, 1998. Article 25 of this comprehensive legislation requires that transfer of personal data take place only to those non-E.U. countries that have an 'adequate' level of privacy protection.[93] This article is designed so as to prevent the circumvention of the Directive and the creation of 'data havens' outside the E.U.

Before entering into an agreement with a foreign country to allow free circulation of personal data outside the E.U., an evaluation of the adequacy of data and privacy protection in that country has to be undertaken. Several countries have already done this including Australia,[94] Switzerland, Hungary, the U.S.[95] and Canada.[96] In the case of the U.S. it has taken a long time to reach an agreement since it relates to a specific system applied in that country known as the 'safe harbour' principle.[97]The safe harbour principle permits U.S. companies to satisfy the European 'adequacy' standard while maintaining their traditional self-regulatory approach to data protection. In July 2000 the European Commission approved the safe harbour framework as meeting the 'adequacy' standard.[98]

Environmental Law

As we are dealing with property ownership and the vertical column of airspace above the land, the question may be asked: Can airspace be owned? Does the person with the title to the land have a proprietary interest in the airspace? If so, will ownership of the land be sufficient to maintain an action in tort? The answer to the first may seem to be yes whereas an answer to the second and third questions may be far more complex as the following cases will demonstrate.

In *Re Lehrer and the Real Property Act* four leases were lodged for registration under the Torrens legislation in New South Wales (NSW). [99] Two of the leases were for upstairs rooms. Jacobs J held that the airspace could be conveyed separately from the soil on which the building was located.[100]

A similar result was reached in the High Court in *Bursill Enterprises Pty Ltd v Berger Bros Trading Co Pty Ltd* where it was held that the grant (which was described as an easement) was in fact a transference of the airspace. [101]

In *Kelsen v Imperial Tobacco Co (of Great Britain and Ireland) Ltd* the plaintiff was a lessee of a tobacco shop. [102] The defendant owned the adjoining building. The defendant attached an advertising sign on the adjoining land, but the sign projected out from the wall by 8 inches (204 mm). The projection resulted in the sign being directly above the roof of the plaintiff's shop. Initially the plaintiff did not object. However, after a commercial disagreement, the plaintiff claimed a trespass and sought a mandatory injunction for the removal of the sign. The issue before the Court was as follows: Was the invasion of the airspace a trespass, or was the plaintiff limited to an action in nuisance? Decision: A trespass was committed. The judge was particularly influenced by the presence of legislation which expressly provided that the flight of aircraft over one's land would not constitute a trespass. Such legislation would be unnecessary if an action in trespass did not lie.

In the case of *Bernstein of Leigh (Baron) v Skyviews and General Ltd* the defendant carried on the business of taking aerial photographs of properties and then offering them for sale to the owners of those properties.[103] Berstein's property was photographed. He responded by suing Skyviews arguing that a trespass has been committed. The issue: Did the passage of the aircraft constitute a trespass? Decision: Griffiths J held that the rights of a landowner should be restricted to such height as is necessary for the ordinary use

[93] Directive 95/46/CE on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, of 24 October 1995, OJ 1995 L 281/31.
[94] Australia, Privacy Amendment Act 2000 (Cwlth) ,22 December 2000; 24 June 2010 <http://www.privacy.gov.au>.
[95] Official Journal of the European Commission L 215 of 25 August 2000. 1, 4 and 7, respectively.
[96]24 June 2010 <http://europa.eu.int/comm/external_relations/canada/summit_12_99/ e_commerce.htm>. and Official Journal of the European Commission L 002, 04/01/2002, p. 0013-6. See also the E.U. 'adequacy' standard agreement at 24 June 2010 <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp39en.pdf>.
[97] "Safe Harbour Principles." 24 June 2010 <http://europa.eu.int/comm/internal_market/en/dataprot/news/shprintiples.pdf>.
[98] Yu, P. "An introduction to the EU Directive on the Protection of Personal Data." 24 June 2010 <http://www.gigalaw.com/articles/2001/yu-2001-07a p1.html >. Harvey JA., Verska, K. " What the European Data Privacy Obligations Mean for U.S. Businesses" <http://www.gigalaw.com/articles/harvey-2001-02-p1.html>.

[99] *Re Lehrer and the real Property Act* (1960) 61 SR (NSW) 365.
[100] McLelland J. in *Depsun Pty Ltd v Tahore Holdings Pty Ltd* (1990) NSW ConvR 58, 902 has held that an "airspace" is not "a legal or equitable estate or interest" in land within the meaning of s 74F of the *Real Property Act 1900* (NSW).
[101] Bursill Enterprises Pty Ltd v Berger Bros Trading Co Pty Ltd[1970-1971] 124 CLR 73.
[102] *Kelsen v Imperial Tobacco Co* [1957] 2 QB 334.
[103] *Bernstein of Leight (Baron) v Skyviews and General Ltd* [1978] 1 QB 479.

and enjoyment of his land and the structures upon it. Above that height, the landowner has no rights in the airspace greater than any other member of the public. In his Honour's opinion, if the Latin maxim were applied literally, a trespass would be committed every time a satellite passed over the land of a suburban garden. The *cujus* principle was not to be taken so literally. The Latin maxim suggests that a person who owns the surface of land also owns the sky stretching to the limits of the atmosphere and all the soil to the centre of the Earth.[104]

In *LJP Investments Pty Ltd v Howard Chia Investments Pty Ltd*[105] the defendant was an owner of property. The defendant was undertaking renovations. Scaffolding extended across to the plaintiff's property. The plaintiff owner seeks a mandatory injunction for the removal of the scaffolding. At issue is this: in applying the *Kelsen* decision, the scaffolding was a trespass, the defendant had acted with callous disregard of the plaintiff's rights, and accordingly it would not be oppressive to grant the injunction. Decision: The Court held that the test is whether the incursion is of such a nature and height as to interfere with the ordinary uses of the land, which an occupier may see fit to undertake. However, the defendant should not use the land of another for their own commercial purposes. A mandatory injunction was granted.[106]

Tort Liability and Nuisance

In the U.S. the tort based upon the right to privacy has been evolving in response to the encroachments upon privacy by the media and others. The U.S. common law of tort has identified four activities that give rise to liability for the invasion of privacy. These are:

- intrusion upon seclusion;
- appropriation of name or likeness;
- publicity given to private life; and,
- publicity placing a person in a false light.[107]

Some states do not, however, recognise such claims; for example, New York does not have a false light claim provision.[108] Other states protect a larger class of persons and private persons, as well as celebrities, such as in California, while New York laws focus on misappropriation of name or likeness.

In the Australian context a new tort for the invasion of privacy has also arisen. In *Grosse v Purvis* a District Court judge recognised a common law right to privacy for the first time in the particular circumstances of a person stalking another.[109] In awarding damages, *Skoien J*. found that the essential elements of the emerging tort of the invasion of privacy were present. These were that the willed act of the defendant intruded upon the plaintiff's privacy in a manner which would be highly offensive to a reasonable person of ordinary sensibilities; and which caused the plaintiff detriment or distress.

An important Australian decision is the protection of privacy under general law.[110] *Lenah Game Meats Pty Ltd* (Lenah) operated a possum meat processing plant located in Tasmania. An unknown person, or people, unlawfully entered the premises and installed video cameras. The video cameras were subsequently retrieved. Video taken of the slaughter and processing of brush tail possums was passed to an animal rights group, *Animal Liberation Ltd*. The group supplied a copy of the video to the *Australian Broadcasting Corporation* (ABC) current affairs program, *The 7.30 Report*. The *ABC* indicated to *Lenah* that it intended to broadcast the video material. Lenah, concerned with the possible negative impact of the video on its business, sought, an interlocutory injunction to restrain the broadcast. While the ABC was not implicated in the unlawful entry, it was clearly aware that the video had been obtained unlawfully, at least following the application for interlocutory relief.

The majority of the Full Court of the Tasmanian Supreme Court extended the principles applied in the previous cases to hold that, absent an enforceable cause of action, an interlocutory injunction could be awarded to restrain publication where it would be unconscionable to use the 'fruits' of an act of trespass. The central legal issue on appeal to the High Court concerned the conditions for awarding an interlocutory injunction. The majority of the High Court rejected Lenah's arguments and held that, in the circumstances, interlocutory relief was unavailable.

A public or common nuisance is an act which interferes with the enjoyment of a right which all members of the community are entitled to, such as a right to fresh air, to travel on highways and so on. A private nuisance is a

[104] Morrison WL, Sappideen C. "Torts. Commentary and Materials." North Ryde: The Law Book Co. Ltd (1993): 92-94.
[105] *LJP Investments Pty Ltd v Howard Chia Investments Pty Ltd* (1989) 24 NSWLR 490.
[106] However, the law remains unsettled. See Price, R., Griggs, L. "Property Law Principle" (2nd ed.) Pyrmont, NSW (2008): Lawbook Co.
[107] Restatement of the Law (Second) Torts § 652A.
[108] *Howell v New York Post Co.,* 596 N.Y.S.2d 350; 612 N.E.2d 699 (Ct. App.) (1993).
[109] *Grosse v Purvis* [2003] QDC 151, 16 June 2003.
[110] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* [2001] HCA 63, 15 Nov. 2001.

tort that is either any wrongful disturbance or interference with a person's use or enjoyment of land or an act wrongfully causing or allowing the escape of deleterious things into another person's land. Nuisance is commonly a continuing injury.[111]

3.1.5.3 Discussion

The Digital Age including the array of social network sites and mobile phones have changed the very notion of privacy. English and E.U. courts seem now more willing to treat as private those activities carried out in public as the *Naomi Campbell* and *Catherine-Zeta Jones and Douglas* cases have demonstrated. Such cases are examples of a statutory tort for the breach of privacy. New causes of action have arisen such as in Australia for an invasion of privacy as shown in the *Grosse v Purvis* and *Lenah Game Meats* cases. These cases have given rise to a reasonable expectation of privacy. However, the advent of CCTV coverage in many modern cities and our movement through public space, while technologically transformative, unfortunately pose a grave threat to personal privacy – variously labelled as locational privacy. Clarke (2008) in advocating Privacy Impact Assessments has observed that deployment of such infrastructure puts the onus back on governments to inform the citizenry of such devices and a failure to do so is a serious shortfall to privacy protection.[112]

3.1.6 Addressing Privacy Issues

It has been asked whether there exists a legal framework in public international law that can cope with the new developments in the Space Age. What might be needed in "... resolving these many challenging legal questions will require creative and flexible solutions as soon as possible" (Jasentuliyana, 2001: 21).[113] What might be needed also is more clarity and precision in defining the issues – something that has not been achieved in the area of privacy protection.

The multidimensional nature of the protection of privacy perhaps has prevented the development of appropriate and holistic privacy protection programme. In the consumer privacy protection arena *al-Shakhouri & Mahmood* (2009) have suggested that the framework may lie in a regulatory approach at both a national and international level as well as a technical approach.[114] Governmental and national efforts in setting up legislation and regulations may help while international efforts are directed towards guidelines such as the 1980 OECD Privacy Guidelines.[115] Technical solutions go to the very technology itself such as 'shutter control' where data collection by satellites might be required to be stopped because of national security, foreign policy and international obligations.[116] In these a balance is required to weight up the economic, social and political payoffs and whether the imposition of conditions and barriers might be disproportionate relative to the low risk of privacy violations.

Slonecker et al. (1998) have suggested that there is a dire need for ethical guidelines to provide the moral philosophy to privacy protection in the absence of a global comprehensive legal and policy framework.[117] On the other hand, von der Dunk (2005) believes that there exists a rudimentary legal framework at an international level mainly in the form of U.N. Conventions, Agreements and Treaties as well as transnational Directives and industry codes of practice.[118] However, at a national level any form of privacy protec-

[111] Legislation in Australia restricts the right of landowners to bring actions for trespass or nuisance in respect of overflying aircraft, e.g., Damage by Aircraft Act 1952 (NSW), s 2(1); Wrongs Act 1958 (Vic), s 30; Damage by Aircraft Act 1964 (WA), s 4; Damage by Aircraft Act 1963 (Tas), s 3; Civil Aviation (Damage by Aircraft) Act 1958 (Cwlth), Schedule. See Bradbrook, AJ, MacCallum, SV Moore, AP (2007) Australian Property Law: Cases and Materials, (3rd ed.) Pyrmont, NSW: LawBook Co. Ltd.

[112] Clarke, R. "Privacy Impact Assessment in Australian Contexts." E-Law Journal 15.1(2008): 73-93. <https://elaw.murdoch.edu.au/archives/issues/2008/elaw_15_1_Clarke.pdf>
Privacy International. "Overview of Privacy." 2007. 28 June 2010 <http://www.privacyinternational.org/article-shtml?cmd[347]=x-347-559062>.

[113] Jasentuliyana, N. "International Space Law Challenges in the Twenty-first Century." Singapore Journal of International and Comparative Law, 5 (2001):10-21.

[114] Al-Shakhouri, NS, Mahmood, A. "Privacy in the Digital World: Towards International Legislation", First Monday, vol. 14 no. 4, 6 April 2009. <http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2146/2153>.

[115] OECD 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Recommendation by the OECD Council of 23 September 1980. 28 June 2010, <http://www.oecd.org/e/droit/doneperso//ocdeprive/priv-en.htm>;<http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-en.htm> , <http://www.oecd.org/documentprint/0,2744,en_2649_201185_15589524_1_1_1_1,00.html>; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 28 June 2010, <http://www.privacy.org/pi/intl_orgs/coe/dp_convention_108.txt>.

[116] Florini, AM., Dehqanzada, YA. "No more Secrets? Policy Implications of Commercial Remote Sensing Satellites.". Carnegie Endowment for International Peace, Carnegie Paper 1 (1999).

[117] Slonecker, EM, Shaw, DM and Lillesand, TM "Emerging Legal and Ethical Issues in Advanced Remote Sensing Technology." Photogrammetry Engineering and Remote Sensing. 64 6 (1998): 589-595.

[118] von der Dunk, F. "Legal aspects of geospatial data gathering in space". GIM International. 19. 8 (2005): 69-71.

tion pertaining to geospatial activities 'barely exists'. This lack of an international framework may be because the basic spatial legal system has been built on the rights and obligations of the States and not the individual. As expressed in the 1986 UN Resolution Principle IV remote sensing activities from space is not to be conducted to the detriment of the legitimate rights and interests of the sensed state. Hence in international space law, the individual has yet to be accorded any rights.[119] This so-called active personal jurisdiction is a long way off from an international personality since it is nascent in its development and is more disputed (von der Dunk 2001).[120] But this may no longer be the case since this very debate on privacy has been narrowed down to its impact on the individual. The commercialisation of remote sensing activities where corporations and private entities have taken over as majority players in deploying satellites and the advent of the Internet now demand that individuals be considered in the equation. Perhaps, as suggested by Ito (2008) it may be time to revisit the UN Principles to put a heavier emphasis on the regulation of remote sensing activities that will remove uncertainties, address the urgent needs for clarification and to establish a more comprehensive regime.[121] Even extant Treaties and Resolutions have shown inadequacies in terms of data policies, liability issues, access to data and third party damage. The principles are also silent on the rights of data generators as well as the rights to intellectual property. Here we may add privacy protection to the list because remote sensing technology is so advanced that individuals may be recognised from high resolution images.

3.1.7 Conclusion

In the U.S. privacy is a fundamental right. Protection of this right in the last half century or so has been based on Fair Information Practices (FIP): collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. A coalition of ten partners from consumer groups and privacy rights has advocated that privacy protection can be achieved when Congress enacts clear legislation that implements Fair Information Practices. Its Legislative Recommendations Primer sets out what is required in regard to protecting individuals, sensitive information, behavioural and personal data, and security safeguards amongst others.[122]

In 2009 the European Space Agency (ESA) member states approved the Sentinel data policy principles that among others established full and open access to data acquisition by Sentinel satellite missions. The Sentinel missions were deployed specifically for the operational needs of the Global Monitoring for Environmental and Security (GMES) programme. One of the key challenges is the legal framework relating to copyright and protection of data, privacy issues and liability for GMES services. A major difficulty is to identify whether GMES services contain or relate to personal data. It has become clear that the GMES programme underlies a very complex legal framework that requires detailed legal analyses, and the establishment of guidelines and models for the legal issues identified above. In addition these legal issues need to be dealt with urgently while not dictating or precluding any particular governance structure.[123]

One wonders now whether geospatial technologies have exposed privacy and whether this exposure has given rise to an unrealistic expectation of privacy protection. Perhaps also privacy has been poorly understood – verging on emotional and mass fear and uncertainty so that calm reflection and contemplation has not taken place. For example, geospatial technology may expose slivers and overlaps in property maps but does not create them. So Eutchev (2005) has suggested that the 'privacy quotient' for GIS is often measured against the user's perception of privacy.[124]

A cynical view is that perhaps the right to be left alone has been steamrolled by the rush of the digital revolution. In so doing privacy may only be available to those who can afford to pay for it.[125] Similarly it has been said

[119] Huikang, H "Space Law and the Expanding Role of Private Enterprises with particular Attnetion to Launching Activities." Singapore Journal of International and Comparative Law 5(2009): 55-62.
[120] von der Dunk, F. "Sovereignty versus space : public law and private launch in the Asian Context". Singapore Journal of International and Comparative Law, 5(2001): 22-47.
[121] Ito, A. "Improvement to the Legal Regime for the Effective use of Satellite Remote Sensing Data for Disaster Management and Protection of the Environment". Journal of Space Law. 34 (2008): 45 – 65.
[122] Center for Digital Democracy, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearninghouse, Privacy times, U.S. Public Interest Research Group, and The World Privacy Forum. Legislative Primer, September 2009. <http://www.uspirg.org/uploads/nE/27/nE27slalKXMxhjOdnoYLEA/Online-Privacy---Legislative-Primer.pdf>.
[123] See discussion by Baumann, I (2009) "GMES Governance. Some Legal Considerations." 28 June 2010 <http://www.bho-legal.com>.
[124] Eutchev, A. "GIS and Privacy". Location Intelligence. 24 March 2005 <http://locationintelligence.net/articles/810.html>.
[125] Given, J. "Privacy is over, get used to it". The Australian Literary Review, 4 March (2009): 10-11.

that privacy is not a right but a privilege, a luxury afforded by wealth and enforced by custom. Most are prepared to trade a bit of privacy for convenience – to save time and money – to divulge personal information in return for discounts, ease of future access and to save time. It may be that the advance of technology and demands of modern business and government have made the traditional ideas of privacy anachronistic.[126]

In discussing legislation for the protection of personal privacy it has been suggested that "… self-regulation is central to maintaining the rights of individuals, the trust of the public, and the economic vitality of the profession and nation as a whole" (Slonecker *et al.* 1998: 594).[127] The problem is to balance the rights of individuals against the rights of the general public to the advantage of all that science now offers in the use of airspace. Hopefully in the discussions above we are working towards a truly *corpus juris spatialis internationalis* (von der Dunk 2001).[128] To have found this we can truly say that we have indeed arrived. But, there is more to be done.

3.2 What Is Privacy?

by Catherine Doldirina

3.2.1 Introduction

Development of surveillance technologies remains a discussion item in democratic societies and includes issues such as to what extent surveillance can be carried out, what purposes it should serve to be justifiable, and others. These and other issues seem to be secondary to the resolution of the question: What is the meaning of the concept of privacy? Protection of privacy is indispensible in any society that respects human rights. Remote sensing activities have seen enormous progress in the past 10 years, and today's satellites can generate data with a resolution of 50 cm. These are data available on the commercial market: one can only wonder what resolution military remote sensing satellites have. The better the resolution of a satellite, the more information can be extracted from the data it generates. This means that if not already, then very soon, remote sensing activities may start impinging on privacy rights.

In order to decide whether a certain activity may compromise privacy as protected in a certain society it is necessary to determine what privacy is. This issue is the focus of this paper. Its aim is to show how multifaceted, diverse and ever-changing privacy is, depending on the structure of society, the time in history or even groups within a given society. It does not attempt to define privacy for regulatory purposes, but calls for taking into account its complexity when regulating any activities that may compromise it. For this purpose the paper explores approaches to defining privacy, as well as the evolution of the concept and its contents over the centuries of human history. Taking from there, it addresses the issues of what the subject matter of protection is and to what extent it is protected. It concludes with some remarks as to the impact of the development of technologies on the concept of privacy and the necessity to address privacy in a regulatory regime.

3.2.2 Approaches to Definition

One of the most characteristic and striking facts about privacy is that it is a concept that easily escapes any precise definition. Privacy is considered to encompass such notions as freedom of thought, control over one's body and personal information, solitude at home, freedom from surveillance, protection of one's reputation, as well as protection from searches and interrogations.[129] Taking into account the multiplicity of interests that privacy is designed to protect, as well as its contribution to sustaining democracy through allowing and fostering development of individuality and creativity, it has been aptly called "the most comprehensive of rights and the right most valued by civilised men."[130]

In today's societies, privacy is indeed recognised as a fundamental human right. The United Nations' Universal Declaration on Human Rights (1948) proclaims that: "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation". This definition allows interpretation of the concept of privacy as a negative

[126] Philipson, G. "Privacy the price of super communication. If you want instant movies, music and phone calls you have no privacy. Get over it". Sydney Morning Herald Next, July 15 (2008): 29.
[127] Slonecker, E.M., Shaw, D.M. and Lillesand, T.M. "Emerging Legal and Ethical Issues in Advanced Remote Sensing Technology." Photogrammetry Engineering and Remote Sensing. Vol. 64 no. 6 (1998): 589-595.
[128] von der Dunk, F. " Legal aspects of geospatial data gathering in space". GIM International. 19 8 (2005): 69-71.
[129] Solove, D.J. "Understanding Privacy." Cambridge: Harvard University Press, 2008.
[130] US Supreme Court Justice Brandeis.

right,[131] although it should be balanced against other negative rights, as well as recognised freedoms.

The definition of privacy, the approach to the legal regime and the focus of the protection it establishes differ and usually depend on the emphasis or the subject-matter of protection that is put forward by the relevant theory. This results in a number of categories of how privacy is defined that are necessary for a better understanding of the range of issues that the concept of privacy encompasses. The first one can be called the right to be left alone or the right of personality: it implies the ability of an individual to determine the extent of the communication of his thoughts, sentiments and emotions to others.[132] The next category focuses on the limitation of access to oneself through the recognition of the value of solitude and of the desire or need to conceal certain things from others: it implies, with slight differences in comparison to the first category, "the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be subject of public observation and discussion"[133] that "entitles one to exclude others from watching, utilising, invading his private realm."[134] The third category can be called 'secrecy' as it primarily focuses on the availability of selective disclosure[135] as to information regarding privacy issues. Another category brings forward the ability of active control over personal information.[136] The two last categories focus on the one hand on personhood, according to which privacy protects irreducible attributes of an individual[137] and, on the other, on intimacy (intimate matters or acts draw "their value and meaning from the agent's love, care or liking"[138]) that stipulates that privacy is essential for human relationships.[139]

Any precise definition of what privacy is or can be also depends on the differentiation between public and private, based on the legal determination of public and private geographical places, as well as of public and private information; on customary expectations and cultural understanding and social perception of public and private; on the accessibility of information to the unenhanced senses; and the actual state of the knowledge.

3.2.3 The Changing Concept

The definitional discussion of the concept of privacy in the previous section showed how different the approaches to defining it and determining its focus can be. Social context is another aspect that plays a crucial role in shaping the concept of privacy, since privacy "obtains its true meaning within social relationships".[140] This is due to the fact that the understanding of both public and private life differs according to particular interpretations - both public and private spheres of life are "fluid and situational or conceptual"[141] A very brief look at the historical facts[142] supports the notion that every era attempts to balance private and public life and determines, according to its dominant values, the amount of private information that can be accessed by the authorities or the society at large. Paradoxically, the dichotomy between the desire to reveal information and the countervailing wish to keep things private remains through time.[143]

In Ancient Greece privacy was not regarded as something worth protecting: "an entirely private life means above all to be deprived of things essential to a truly human life: to be deprived of the reality that comes from being seen and heard by others, ... or to be deprived of the possibility of achieving something more permanent than life itself."[144] In Ancient Rome, meanwhile, there was a clear distinction between public (*publicus*) and private (*privates*), and the private sphere

[131] Sofsky, W. "Privacy: A Manifesto." Rendall. S transl. (Princeton University Press: Princeton & Oxford, (2008):30.
[132] Warren, S., Brandeis, L. "The Right to Privacy." Harvard Law Review, 4 (1890): 193.
[133] Godkin, E.L. "Libel and Its Legal Remedy." Journal of Social Science 12 (1880): 69-80.
[134] Van Den Haag, E. "On Privacy, in Nomos XIII: Privacy "J. Roland Penncock & J.W Chapman eds., 1971. 149.
[135] Karst, K.L.. "Legal Controls over the Accuracy and Accessibility of Stored Personal Data. 31 Law and Contemporary Problems ."(1966):342, 344.
[136] Fried. Charles. "Privacy".Law, Reason, and Justice: Essays in Legal Philosophy .Graham B. J. Hughes ed., New York: New York University Press, 1969. Note that the major problem with this category is that privacy is not simply a subjective matter of individual prerogative, but also an issue of what society deems appropriate to protect
[137] Freund, P. Address at the American Law Institute 52nd Annual Meeting 42-43 (1975).
[138] Inness, J. "Privacy, Intimacy and Isolation". New York: Oxford University Press (1992):73.
[139] With the problem that some private things, like bank account information, are private but not intimate.
[140] Gutwirth, S. "Privacy and the Information Age". Casert, R. trans. (Lanham/Boulder/New York/Oxford: Rowman & Littlefield Publ. 2002) at 34.
[141] Marx, G. Murky Conceptual Waters: The Public and the Private. 3 Ethics and Information Technology 157 (2001).
[142] For more details *see* Sofsky, W. *Privacy: A Manifesto* at 25-29. For a very extensive overview s*ee* Veyne, P. *History of Private Life* in 5 volumes. Belknap Press, 1992.
[143] Keeler, M.R. "Nothing to Hide: Privacy in the 21st Century." Lincoln: Universe, 2006.
[144] Arendt, H. "The Human Condition." Chicago: University of Chicago Press, 1958. 58.

was outside the scope of any regulations.[145] At the same time the life of political figures was very open and every step they made, including marriage or a will, was evaluated by public opinion. In Europe, the Renaissance and Christianity had a different – more intrusive – attitude towards privacy, which was manifested in *e.g.* regulations regarding the construction of private houses, declarations of wealth, rules of marriage and even obligations as to dress code. The French Revolution reduced the private domain even more, but not through the Church and religion as before, but through municipal institutions.

Today, although privacy and its protection are considered to be essential to normal life, modern technologies and, for instance, the development of social networks provide for a great exposure of information that one would think is absolutely private. In addition, even in the same time period different societies may understand and value privacy differently, as for example with the issues of the boundaries of personal space - the concept of personal space varies across nations, yet members of a particular culture have a precise sense of over-familiarity.[146]

3.2.4 Why Protect?

Several arguments come to support the protection of privacy. In today's reality probably one of the most important is the essentiality of privacy for democracy, as it fosters and encourages the central requirement of current regimes, "the moral autonomy of the citizen"[147], and influences social structures, power, and freedom. Furthermore, the concept of privacy is based on and recognises the moral duty to respect an individual's dignity and autonomy. It reflects the importance of autonomous life and personal integrity. Privacy prevents establishment of too much social control that can negatively impact freedom, creativity and self-development. In the long run, privacy emphasises and reinforces trust within a society[148] in that it teaches its members to interact without having all possible information about each other. Privacy protects aspects of individuality that have a high social value; it not only protects individuals but also fosters social interests. Privacy is also important because of security issues, as it prevents unnecessary exposure.

Promoters of a wider availability of private information argue, to the contrary, that privacy lessens society's ability to detect and punish disobedience, which complicates the law enforcement process.[149] They believe that privacy can also impede commercial efficiency and profitability in that it will be more difficult for companies to collect, store and use information upon which they base business decisions.[150] Importantly, privacy may conflict with the free flow of information and other societal values and goals, like prevention and detection of crime and national security. From this perspective, even if privacy is seen as a negative right, it needs to be assessed together with other rights and freedoms, and to be reconciled with other individual rights.[151]

3.2.5 What to Protect?

The aspects of our private life that a privacy regime protects can be classified content- and subject-wise. In terms of content, privacy protects family, body, sex, home, and communications. With regard to the specific activity, privacy protects the content of private life from actions such as invasion into the private realm, as well as the collection, processing, and dissemination of information.[152] One of the major challenges that policy-makers and regulators face is to determine whether and what information is private or public. The decision should take into account the purposes for which people want to conceal certain data and the uses that others might make of them in case access is granted. Another important issue that has to be assessed is the fact that people often may trade privacy "for convenience or to bargain the release of personal information in exchange for relatively small rewards".[153] Imposition of such choices on them through regulations should not be allowed.

The understanding of privacy often determines the subject-matter of the regulations that build the relevant legal framework. The most vivid examples of the differences in

[145] It was manifested in the absence of state religion, free transfer of property and in availability of divorce to both sexes.
[146] Supra 129, 40.
[147] Gavison, R. "Privacy and the Law." Yale Law Journal 89, Vol.3 (1980): 455.
[148] For the opposing view that privacy can impede establishment of truth, and therefore trust to each other and judgement of people's reputations, in Walker, K. "The Costs of Privacy." Harvard Journal of Law and Public Policy 25 87 (2002): 91.
[149] Rule, J.B. "Private Lives and Public Surveillance: Social Control in Computer Age." 1974. 21-22.
[150] Cate, F.H. "Privacy in the Information Age." Washington, D.C.: Brookings Institution Press, 1997. 28-29.
[151] Etzioni, A. "Limits of Privacy." New York: Basic Books, 1999.
[152] Baase, S. A. "Gift of Fire: Social, Legal, and Ethical Issues for Computing and Internet." 3rd ed. Upper Saddle River, New Jersey: Pearson Education, 2008.
[153] Acquisti, A., Grossklags, J. "Privacy and Rationality in Strandburg.", K. & Raicu, D.S. eds. Privacy and Technologies of Identity: A Cross-Disciplinary Conversation New York: 2006. 15-16.

approaches to privacy, both theoretical and practical, can be illustrated by comparing those in Europe and the US. In the US privacy is seen as a part of liberty and the main focus of privacy protection is from or against governmental encroachment into the private realm. In Europe, by contrast, the regulations are based on the recognition of privacy as a human right and are therefore much more concerned with protecting individuals from undesired exposure[154] rather than from the government[155] that enjoys more trust than in the US. These foundations have quite far-reaching implications both on the level of law-making[156] and law-enforcement: some of them are highlighted in this section.

Privacy protection regarding consumer data is one example of the impact of different approaches to regulating privacy issues, which is increasingly gaining attention particularly with the development of internet technologies. Allegedly, consumer "data stalking and information trafficking" are considered as part of normal business activities in the US.[157] The reasoning in favour of allowing these practices is that they lower the costs for buyers and sellers to find each other, which in the long run enhances market efficiency. On the contrary, this approach is precluded in Europe where free-market arguments are not dominant when adopting legal norms regarding privacy protection. In this regard, the purchase of consumer preferences data by marketers is not allowed as it may seriously violate the privacy rights of consumers.[158] This clash of approaches led in the 1990s to a conflict between the two jurisdictions that was resolved only in 2000 through the so-called 'safe harbour' agreement that aimed at reconciliation of the two approaches and provision of more protection to European consumers.[159]

Another example of the difference in focus as to what privacy should protect is the gathering and availability of financial information. In Europe it is not easily available, apart from information about insolvents and bankrupts. Moreover, it is usually gathered either by public bodies (as in France) or specially designated organisations (like in Germany) and can be used only for the purposes laid down as acceptable by relevant regulations. In the light of European practices, the situation in the US is quite the opposite, since making compilations of an accessible record of any individual's credit history is allowed.[160]

3.2.6 Protect – to What Extent?

The degree of necessity of protecting certain aspects of the private lives of citizens changes, and another example from Ancient Greece illustrates this perfectly: for the Greeks, the naked body was an attribute of a civilised person, as public nudity "affirmed one's dignity as a citizen".[161] It therefore needed no protection whatsoever, which is unthinkable today. In general, even in societies that exist at the same time, practices regarding any privacy sphere have numerous variations depending on such factors as urbanisation, class and social status, ethnicity and religious beliefs. Without doubt, what is public and private is shaped by culture and history. In this context, the question as to how flexible the relevant regulations have to be becomes relevant. If the extent of protection of privacy is a variable, then we need some principles that remain relatively constant and are used to determine the shape of the variable – the available protection.

The most widely used assessment criteria to determine what information should be denied access to by the public at large and to guide the activities of both legislators and law-enforcing institutions can be categorised in two groups. The first category encompasses criteria referred to as 'private' and signifies individual choice of what to "withdraw from public view".[162] This approach is problematic in application as it is virtually impossible to adopt a workable system of protection around such a conception of privacy: it varies with each individual's idiosyncrasies. The second category brings forward the notion of 'reasonable expectation of privacy' in order to determine the amount of protection granted by the regime. Its advantage over the first category lies in the fact that its assessment criteria are not linked solely to the individual's particular expectations, but incorporates those that a society considers appropriate. This concept is very often applied by courts across the globe, including the European Court of Human Rights (ECHR).

[154] *Whitman.* Ford Foundation Professor of Comparative and Foreign Law, Yale.
[155] Reidenberg, Joel R. "E-Commerce and Trans-Atlantic Privacy." (2001) 38 Hous. L. Rev. 717-731.
[156] In the U|S, unlike Europe, there is no 'constitutional' law that lays down general principles of the protection of privacy.
[157] Joel R. Reidenberg Professor of Law. Fordham University School of Law.
[158] Supra 154.
[159] Whitman, J.Q. "The two Western cultures of privacy: dignity versus liberty." Yale Law Journal 6, Vol. 113, April 2004. 1151.
[160] Ibid.
[161] Sennett, R. "Flesh and Stone: The Body and the City in Western Civilisation." W.W New York: Norton & Company Inc, 1994. 33.
[162] Young, I.M. "Justice and the Politics of Difference." Princeton: Princeton University Press, 1990. 119-120;

As highlighted in the previous sections, the determination of privacy depends on many factors. In Europe, for instance, unlike in the US,[163] the law offers protection to privacy in various realms of life, whether the issue is consumer data,[164] credit reporting,[165] work-place privacy,[166] discovery in civil litigation, or protection of criminal offenders from public exposure.[167] Similarly, in many countries the laws and regulations do not protect privacy once a person leaves his own house[168] and enters public spaces such as streets.[169] These differences are sometimes explained through the concepts of 'data protection', which is narrower and is used in the USA, and 'protection of information privacy', which is broader and serves as a basis for regulations in the EU.[170]

3.2.7 Impact of New Technologies

The development of (surveillance) technologies has a twofold effect on the treatment of privacy issues. On the one hand, it enables some researchers to argue that interests such as freedom from police 'coercion' or use of force should be specifically preserved rather than a broad concept of privacy as such. On the other hand, others propose that privacy concepts should be narrowed down to only the most offensive governmental invasions. Changes in the regulations can also arise from the expectations of individuals such as, for instance, in the case of consumer protection: consumers from countries with some government regulation of information privacy desire even stronger regulation of data collection,[171] unlike consumers from countries where no or very little protection is available.

At the same time, technology may play a role in shaping people's expectations as to what behaviour is appropriate in society. For instance, services like Google maps and street view may, due to their ability to unexpectedly expose persons on a global scale, in the long run force good behaviour. Such practices may further contribute to the stronger realisation of the necessity of distance among members of a society and as a result protect them from false intimacy and false community.[172]

The major danger the technological development has brought is reduction of the costs of data collection, which has led to a situation of accumulation of too much (sometimes unnecessary) data.[173] In addition, the modes of data storage and accessibility have changed dramatically and may affect the ways of protecting privacy as well. For instance, interactive maps available for a range of uses that integrate remote sensing satellite data into geographic information systems (GIS) may reduce the private realm available to us today. GIS technology enables users to link limitless types of data (ranging from census data to crime statistics) on a certain activity to mapping software.[174] The implication of this is that zooming in a particular image within a GIS may reveal all personal or other information that is linked to this geographic location.[175]

3.2.8 Conclusion

This sketch on privacy has hopefully highlighted several issues. First of all, privacy is a complex, definition-escaping concept that is very much shaped by the habits and the culture in a given society and may change over time and even within different social layers of the same society. Secondly, different societies may and do adopt varying approaches to

Whitman, J.Q. "The two Western cultures of privacy: dignity versus liberty." Yale Law Journal 6, Vol. 113, April 2004. 1151

[164] Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31;Scheer, D. "Europe's New High-Tech Role: Playing Privacy Cop to the World." Wall Street. Journal 10 October 2003: A1.

[165] Wuermeling, U. "Scoring von Kreditrisken." N.J.W. 55 (2002): 3508. Noting that credit scoring is provided only through statistical aggregation of anonymized data, in order to prevent violations of the privacy rights of individual consumers.

[166] For an analysis of the differences between German and the US approach to the issue, see Finkin, M.W. Menschenbild. "The Conception of the Employee as a Person in Western Law." *23* Comp. Lab. L. & Pol'y J. (2002): 577.

[167] Whitman, J.Q. "Harsh Justice: Criminal Punishment and the Widening Divide between America and Europe." New York: Oxford University Press, 2003. 84-92.

[168] Although this is the focal point of protection in the US – privacy in one's house. See Boyd v. United States, 116 U.S. 616, 630 (1886).

[169] Taslitz, A.E. "The fourth Amendment in the Twenty-First Century: Technology, Privacy and Human Emotions." Law and Contemporary Problems 65.2 (2002): 125-187.

[170] Bellman, S. "International differences in Information Privacy Concerns: A Global Survey of Consumers." The Information Society 20 (2004): 313-324. These differences stem from the philosophy behind understanding what privacy is designed to protect: dignity in Europe and liberty in the US. See Post, R.C. "Three Concepts of Privacy." GEO. L.J. 89 (2001): 2087.

[171] Bellman, S. "International differences in Information Privacy Concerns: A Global Survey of Consumers." The Information Society 20 (2004): 313-324

[172] Supra 131, 45.

[173] "Privacy International Responds to European Commission Consultation on the Privacy Directive of 31 Dec. 2009." <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-565803>.

[174] More info online: <www.gis.com>.

[175] Privacy International. "Threats to Privacy. (October 28, 2006). Online: <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-543674>.

defining and protecting privacy, which in the contemporary globalising world leads to clashes of both a regulatory and an enforcement nature. In addition, often the theory chosen to govern the legal framework of privacy protection influences its subject matter, focus and the extent of the protections granted. Lastly, the rapid technological development of today may pose new and unexpected issues that have to be tackled or addressed in order to maintain the desired level of privacy protection.

This said, it is necessary to point out that despite all the differences in approaches to define privacy and establish a regime for its protection, a lot of things discussed and brought up in this paper and in the research that serves as its basis are neither universal nor 'hopelessly'[176] variable. Most of the issues, principles and rules lie in between the two and have many shared attitudes towards them across jurisdictions. The similarities in treating issues regarding privacy across jurisdictions should be used as the basic principles on which to build effective regulations.

3.3 The European Convention on Human Rights and EU Law – Two European Legal Approaches to Privacy, as Relevant to High-Resolution Imaging

by Frans von der Dunk

3.3.1 Introduction

The recent, sometimes major strides in the development of Very-High Resolution (VHR) remote sensing satellites have led to remote sensing products of sub-meter resolution being commercially available, and the expectation that this resolution will continue to become better over the next few years. This development, it seems, may soon start interfering with the privacy of individuals and individual entities, not just with the 'privacy' of states.[177]

Europe, with major governmental and intergovernmental players in the remote sensing area as well as a few renowned private remote sensing data providers, is one of the regions where legal issues pertaining to such a potential interference with privacy will have to be dealt with. Thus, the question has often been broached which this paper briefly tries to survey: what, if any, would be the 'European approach' to these issues?[178]

It may be pointed out at the outset, that in the four UN treaties widely considered the core of the *corpus juris spatialis internationalis,*[179] the issue of privacy as such was not at all dealt with. In consequence, the issue can only be approached from the point of departure of the law on privacy. However, before moving to the substance of mapping how in Europe the issue of protecting privacy as it is relevant in the context of space-based VHR remote sensing data has been dealt with, with respect to any possible 'European approach' beyond the level of individual national jurisdictions, it should be noted that more than one intergovernmental European entity plays a key role in this context.[180]

From a strictly space-based perspective, perhaps analysis should first address the European Space Agency (ESA),[181] Europe's standard-bearer in space in general terms and/or EUMETSAT,[182] Europe's standard-bearer in

[176] Supra 129.

[177] Gaudrat, P., Tuinder, P.H., "The Legal Status of Remote Sensing Data: Issues of Access and Distribution". Lafferranderie, G., Crowther (Eds.). Outlook on Space Law over the Next 30 Years (1997), 353-6; Jackson, S.M. "Cultural Lag and the International Law of Remote Sensing". 23 Brooklyn Journal of International Law (1998):856-860.

[178] For those interested in the full details of the analysis, reference may be had to the author's Europe and the 'Resolution Revolution': 'European' Legal Approaches to Privacy and their Relevance for Space Remote Sensing Activities, 34 Annals of Air and Space Law (2009) : 809-844.

[179] This concerns the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, London/Moscow/Washington, done 27 January 1967, entered into force 10 October 1967; 610 UNTS 205; TIAS 6347; 18 UST 2410; UKTS 1968 No. 10; Cmnd. 3198; ATS 1967 No. 24; 6 ILM 386 (1967); the Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, London/Moscow/Washington, done 22 April 1968, entered into force 3 December 1968; 672 UNTS 119; TIAS 6599; 19 UST 7570; UKTS 1969 No. 56; Cmnd. 3786; ATS 1986 No. 8; 7 ILM 151 (1968); the Convention on International Liability for Damage Caused by Space Objects, London/Moscow/Washington, done 29 March 1972, entered into force 1 September 1972; 961 UNTS 187; TIAS 7762; 24 UST 2389; UKTS 1974 No. 16; Cmnd. 5068; ATS 1975 No. 5; 10 ILM 965 (1971); and the Convention on Registration of Objects Launched into Outer Space, New York, done 14 January 1975, entered into force 15 September 1976; 1023 UNTS 15; TIAS 8480; 28 UST 695; UKTS 1978 No. 70; Cmnd. 6256; ATS 1986 No. 5; 14 ILM 43 (1975).

[180] R. Harris, "Earth Observation and Principles on Data." Law and Geography – Current Legal Issues 5 (2002), 544-546

[181] ESA was established by the Convention for the Establishment of a European Space Agency, Paris, done 30 May 1975, entered into force 30 October 1980; 14 ILM 864 (1975); Space Law – Basic Legal Documents, C.I.1.

[182] EUMETSAT was established by the Convention for the Establishment of a European Organization for the Exploitation of Meteorological Satellites (EUMETSAT), Geneva, done 24 May 1983, entered into force 19 June 1986; as

space-based meteorological remote sensing.[183] Both, however, are intergovernmental organisations, not regulatory but operational in nature, and therefore involved in dealing with privacy issues in a legal sense only through contracts concluded with downstream data collecting and distributing entities – in other words: very much an *ad hoc* approach.

From a legal and regulatory perspective, therefore, of much greater importance for analysing the European 'spacescape', would be the two approaches taken by two international entities which do focus on regulation, even legislation in a proper sense – even if hardly focusing on regulating or legislating space activities. This concerns on the one hand the Council of Europe, not to be confused with the Council of Ministers or European Council (both institutions of the European Union), and on the other hand the European Union, especially now that the Treaty of Lisbon[184] has provided the latter with a first comprehensive measure of competence in the space area.[185]

3.3.2 The Council of Europe, the European Convention on Human Rights and Privacy

The Council of Europe was established as early as 1949, in an effort essentially to provide legal instruments to try and prevent the atrocities against civilians in general perpetrated by the Nazis and their allies from recurring again.[186] Consequently, its major achievement was and is the European Convention on Human Rights.[187]

The European Convention followed on the heels of the United Nations-developed Universal Declaration on Human Rights of 1948, which represented the first official global catalogue of modern-day human rights. The Declaration thus already provided for a prohibition on arbitrary interference with privacy and the basic requirement of establishing adequate protective legal instruments in the national context to underpin that prohibition.[188] On the international level, the Declaration was followed up by the International Covenant Civil and Political Rights, which similarly – this time in legally binding fashion and underpinned by a dispute settlement system – provided for the prohibition of arbitrary interference with privacy and the entitlement of individuals to protection by law against such interference.[189]

Yet, the European Convention on Human Rights was first in achieving that same level of legislative institutionalisation on the international level, as applicable *ipso facto* to all member states of the Council of Europe. The key article in the Convention dealing with privacy is Article 8, which reads in full:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Thus, essentially only the cumulative fulfilment of two conditions could justify interference with privacy: (1) such interference should be appropriate and proportional, justified by overriding concerns of a public nature of sufficiently important nature, and (2) such interference should also be specifically allowed by law, so as to allow sufficient legal certainty and preclude any use of the argument of 'appropriateness' to *ad hoc* circumvent privacy protection rules.

A number of key cases since 1953, the year of the entry into force of the Convention, further elaborated and deepened the specific understanding and application of this clause. Two cases, both of 2002, are most important with a view to impact on the use of satellite

amended 14 July 1994, entered into force 27 July 1994; Cmnd. 9483; Space Law – Basic Legal Documents, C.III.1; 44 ZLW 68 (1995).

[183] Note that, while ESA and EUMETSAT are related in practical terms in many ways, their membership substantially differs: ESA currently counts 18 member states, EUMETSAT 26 member states.

[184] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (hereafter Treaty of Lisbon), Lisbon, done 13 December 2007, entered into force 1 December 2009; OJ C 306/1 (2007).

[185] Art. 189, Treaty establishing the European Community as amended by the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, Lisbon, done 13 December 2007, entered into force 1 December 2009; OJ C 115/47 (2009). Further already e.g. S. Hobe et al., "A New Chapter for Europe in Space." Zeitschrift für Luft- und Weltraumrecht 54 (2005): 346.

[186] Statute of the Council of Europe, London, done 5 May 1949, entered into force 3 August 1949; ETS No. 001. The Council of Europe currently counts 47 member states, covering more or less all of the geographical continent of Europe.

[187] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, done 4 November 1950, entered into force 3 September 1953; ETS No. 005.

[188] Art. 12, Universal Declaration of Human Rights, Paris, UN GA Res. 217 A (III) of 10 December. A/RES/217.

[189] Art. 17, International Covenant on Civil and Political Rights, New York, done 19 December 1966, entered into force 23 March 1976; 6 ILM 368 (1967).

remote sensing data resulting in potential interference with privacy.

The first of these concerns the *Pretty case,*[190] which actually elaborated on two key issues. Firstly, Article 8 (in contrast to, for example, the applicable provisions of the International Covenant on Civil and Political Rights) as such only referred to obligations resting upon governmental authorities to desist from interference with privacy. This raised the so-called 'paparazzi-problem', where in Europe threats to privacy are often considered to be more likely and/or a nuisance when stemming from private sources, read the media, than from the government. In the *Pretty case*, the European Court of Human Rights (the ultimate court to adjudicate on those issues under the Convention) made it clear however that Article 8 should be read as also including a 'positive obligation' of public authorities to ensure adherence to privacy protection by other individuals or private entities within their respective jurisdictions.

The other issue for which the *Pretty case* is particularly known concerned the protracted debate on the precise definition and scope of the concept of 'privacy' under the Convention. Though the Court, further to earlier, not entirely successful efforts by others,[191] did not exhaustively define 'privacy', it noted that this was to be considered a very broad concept, covering at the least such aspects as personal autonomy, physical and psychological integrity, and often extending to physical and social identity questions.[192] Any intrusion, whether actual and physical or virtual and psychological, in the personal domain could thus, in principle, be assessed to constitute a violation of Article 8.[193] The broadness of the definition also certainly allows, in principle, the inclusion of certain remote sensing activities as intruding upon such autonomy or identity.

The other case of concern here was the *Colas Est case.*[194] In this case, it was confirmed by the European Court of Human Rights that the right of 'privacy', however defined, in principle would not only be available to individuals, but also to juridical persons such as private companies. This conclusion is especially important in the light of increasing discussion of, or even implementation of, the use of VHR remote sensing data for example for detection of violation of laws on environmental pollution or the growing of certain crops, both on a national level and on an EU level.[195]

Further potential relevance of this particular European regime dealing with privacy for remote sensing would stem from concerns in the context of the Convention's regime and its application with registration of personal data, as a vital issue for privacy concerns in view of the quasi-omnipresence of electronic storing devices and the Internet.[196] Once remote sensing data would become sufficiently detailed to present a threat to interfering with privacy (if not, indeed, they sometimes already are) such issues may crucially interfere with the interest of remote sensing data providers to share their data as widely as possible – whether against a fee, as with commercial providers, or as an element of public information or general benefit, as with the GMES programme being developed by the European Union and ESA.[197] It may be

[190] *Pretty v. The United Kingdom* (Application no. 2346/02, Judgment of 29 April 2002); see further P. van Dijk et al (Eds.), "Theory and Practice of the European Convention on Human Rights" 4th ed., (2006): 664-665.

[191] e.g. J. Velu. "The European Convention on Human Rights and the Right to Respect for Private Life, the Home and Communications." Privacy and Human Right. Ed A.H. Robertson. 1973. 32-33.

[192] Pretty case, at § 61.

[193] Purdy, R. "Legal and Privacy Implications of Spy In The Sky Satellites." Mountbatten Journal of Legal Studies 3 (1999): 65-75; Macrory R. and Purdy, R. "The use of satellite images as evidence in environmental actions in Great Britain." Droit et Ville 51 (2001): 84-7.

[194] *Colas Est v. France* (Application nr. 37971/97, Judgment of 16 April 2002).

[195] Ginzky, H. "Satellite images as evidence in legal proceedings relating to the Environment. A US perspective." Droit et Ville 51 (2001): 44.; Macrory, R. Purdy, R. 73 ff.; Molteni, F. "Use of Earth Observation Data as Evidence in Judicial Proceedings Concerning Environmental Infractions: The moot Court Test." Droit et Ville 51 (2001): 115+.; Levanthis, E.N. "Forest Protection and Illegal Development of Settlements in Forests and Forest Areas." Droit et Ville 51 (2001): 131+. Cf. also on international environmental treaties e.g. N. Peter, "The Use of Remote Sensing to Support the Application of Environmental Treaties". Proceedings of the Forty-Sixth Colloquium on the Law of Outer Space, 29 Sep. – 3 Oct. 2003, Bremen, Germany. 74-80. Relevant European legislation includes Council Regulation establishing an integrated administration and control system for certain Community aid schemes, (EEC) No 3508/92, of 27 November 1992; OJ L 355/1 (1992); and Commission Regulation laying down detailed rules for applying the integrated administration and control system for certain Community aid schemes, (EEC) No 3887/92, of 23 December 1992; OJ L 391/36 (1992).

[196] Tahu, G.J., Baker, J.C. and. O'Connell, K.M., "Expanding global access to civilian and commercial remote sensing data: implications and policy issues." Space Policy 14 (1998): 184.

[197] European Council Resolution on the launch of the initial period of global monitoring for environment and security (GMES), of 13 November 2001; OJ C 350/4 (2001); Communication from the Commission to the European Parliament and the Council – Global Monitoring for Environment and Security (GMES): Establishing a GMES capacity by 2008, COM (2004) 65 final, of 3 February 2004; Communication from the Commission to the Council and the European Parliament – Global Monitoring for Environment and Security (GMES): From Concept to Reality, COM(2005) 565 final, of 10 November 2005; Harris, Further R., Browning, R. "Global Monitoring for Environment and Security: data policy considerations." Space Policy 19 (2003): 265-276; Muñoz Rodriguez, M.C & J.M., de Faramiñán, Gilbert.

pointed out, for example, that under the INSPIRE Directive[198] EU member states are specifically obliged to guarantee that electronic networks are available for the purpose of sharing certain types of geographic information as widely as possible.

Also, the question of whether respect for the home and protection against nuisance in the enjoyment of one's home would be at stake in case of 'intrusion' by satellite, in particular when taking place the context of private companies and their 'homes', may have to be addressed sooner rather than later – with obvious reference to a body of case law existing already on such forms of intrusion by aerial photography or other non-physical means of intrusion.[199]

It should be added, finally, that under the European Convention on Human Rights in certain circumstances applicable rights, including those concerning privacy, may be temporarily suspended by proper legislative means – notably, these concern cases of war, public emergencies, national security and public safety. This in particular may be an area worthy of further study with a view to GMES, as focusing on a whole range of public security applications.

3.3.3 The European Union, EU Law and Privacy

Whilst for the European Convention on Human Rights, as developed in the context of the Council of Europe, privacy was exclusively addressed as a matter of human rights, the other legal regime to be scrutinised here becomes involved in privacy not from a human rights but from an economic perspective. In other words, true to its original mission to establish a free trade area and a level playing field for private commercial and economic activities, the European Community, then Union, started to involve itself with privacy issues once these were seen to start to interfere with developments towards the Internal Market, and the free and open competition envisaged therein.[200]

Thus, it was essentially the ever increasing trans-border flow of personal data as a main element of the modern European economy and based on electronic services or services using electronic means, which raised the issue – and in principle did not exclude data generated by satellites from their scope: to what extent should increased risks of interference with privacy as a consequence of such data streams lead to limitations to the generation, distribution and/or use of such data, inevitably limiting economic opportunities available to entrepreneurs in this context?

As a point of departure, it should be noted that also the European Union is bound by international human rights law, including notably the European Convention on Human Rights – from the outset already because all its member states, all also parties to the Convention, could not dodge their obligations under it by transferring any relevant legal authority to the Community/Union organs, then because the Union as such became a party to the Convention.[201]

Still, for the Union that did not take away the need to try and establish a proper balance between privacy concerns and free-trade-related concerns, leading – within a few years after the fundamental establishment of the Internal Market by the Treaty on European Union[202] – to the Data Protection Directive[203] being enunciated in 1995.

The Directive confirms the basic dichotomy of the EU approach: that on the one hand EU member states shall protect human rights to privacy however defined and delineated by other applicable legal regimes, but on the other hand shall – at least in principle – neither restrict nor prohibit the free flow of personal data if that unduly interferes with the Internal Market and free and open competition. From this, an approach results which has as its overarching aim to provide *equivalent* protection, rather than, as such, a high or low level of protection – since widely dif-

"The Cooperation Between ESA and EU Regarding the Earth Observation." Proceedings of the Forty-Ninth Colloquium on the Law of Outer Space, 2-6 Oct. 2006,Valencia, Spain. 198-201.

[198] Directive 2007/2/EC on establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) of 14 March 2007. OJ L 108/1 (2007); further e.g. L.J. Smith, C. Doldirina. "The EU INSPIRE Directive: a Suitable Mechanism to Make Spatial Data." Proceedings of the Fiftieth Colloquium on the Law of Outer Space, 24-28 Sept. 2007 Hyderabad, India.109-18.

[199] See already Purdy, esp. 76-77.

[200] Art. 3 (3) of Treaty on European Union as amended by the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, Lisbon, done 13 December 2007, entered into force 1 December 2009; OJ C 115/1 (2009), providing that "[t]he Union shall establish an internal market" as one of its key aims.

[201] Consequently, Art. 2, Treaty on European Union as amended by the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, provides that "the Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights". Cf. also Art. 3(2).

[202] Treaty on European Union, Maastricht, done 7 February 1992, entered into force 1 November 1993; 31 ILM 247 (1992); OJ C 191/1 (1992).

[203] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 24 October 1995; OJ L 281/31 (1995).

fering levels of protection of privacy within the various member states would 'unlevel' the playing field and distort competition within the Union as a whole.

The Data Protection Directive addresses the issue through the key concept of 'personal data', reshaping the privacy concept to a set of items the handling of which may interfere therewith. 'Personal data', then, are defined by the Directive as:[204]

> [A]ny information relating to an identified or identifiable natural person hereinafter referred to as 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

The essence of the legal regime then applied to such personal data under the Directive provides that they may be collected, processed and distributed or allowed to be accessed if they were processed fairly and lawfully, if they were collected for specified, explicit and legitimate purposes (and only used for those), if they are accurate, and if either the so-called 'data subject' has unambiguously consented or processing would be necessary for purposes specified by law (respectively as a consequence of legal obligations resting upon the data subject itself).[205]

The above clauses are applicable to cases where the data subject itself provides the data; if data are however somehow not so obtained, in addition the data subject has to be informed of the processing of data and the substance thereof, as well as of the identity of the 'data controller' and the rights of access and rectification accruing to the data subject, in order for data collection, processing and distribution to be allowed.[206]

Though phrased differently from the European Convention on Human Rights' Article 8 on privacy and thus potentially still giving rise to conflicting interpretations and implementation in specific cases, this provision largely reflects the basic twofold requirement for allowing interference with privacy, as summarised before: (1) such interference should be appropriate and proportional, justified only by overriding concerns of a public nature of sufficiently important nature, and (2) such interference should also be specifically be allowed by law in clear and unequivocal terms.

Article 8 of the Directive in any event prohibits the processing of data if these would be revealing racial or ethnic origins, political opinions, personal beliefs, trade-union memberships, personal health or sex life of an identified or identifiable individual and so on. By contrast, the aforementioned limitations to the use of personal data do not apply if they are to be used for statistical, historical and scientific purposes – as long as no individual persons could be identified as a consequence of that use.[207]

Another set of exceptions from the application of the EU-wide system of protection of privacy is provided by Article 3: no prohibitions to use under the Directive apply if such use is for purposes of public or state security, defence, or state activities in areas of criminal law. This, however, essentially means that *national* restrictions may – and would rather likely – still apply; state security and criminal law still form part of national member state's sovereign domains outside the scope of EU law.

Further to the Data Protection Directive, a few EU law documents have addressed subsets of privacy-related issues. Thus, Regulation 45/2001[208] applied the Data Protection Directive specifically to the European Union itself and its institutions – which in view of the possible role of the Union itself or an EU agency in GMES may have special relevance also for the European remote sensing 'spacescape'. Directives 97/66[209] and 2002/58,[210] the later amending the former so as to take account of the convergence of information and computer technology, deal with privacy issues specifically in the context of telecommunication services and the role of the publicly available and accessible telecommunications infrastructure in such services, for example by elaborating on wiretapping prohibitions. Finally, Decisions 497/2001[211] and 16/2002[212] deal with the

[204] Art. 2(a), Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 24 October 1995; OJ L 281/31 (1995).
[205] Ibid. Artt. 6-7.
[206] Ibid. Art. 11.
[207] Ibid. Art. 11.
[208] Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data of 18 December 2000; OJ L 8/1 (2001).
[209] Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector of 15 December 1997; OJ L 24/1 (1998).
[210] Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2002; OJ L 201/37 (2002).
[211] Commission Decision 497/2001/EC on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, of 15 June 2001; OJ L 181/19 (2001).
[212] Commission. Decision 16/2002/EC on standard contractual clauses for the transfer of personal data to proces-

application of the EU regime outside of the Union itself, that is essentially as applicable to activities of EU companies and other entities (GMES operators, for example) outside the Union's territory.

From the perspective of VHR remote sensing, it is noteworthy firstly that in the case of satellite data generation and procession of such data the data subjects usually are not involved, or even aware, which means the requirements regarding their awareness and consent would be at issue.[213] This might of course result in major obstacles for these operations if it would mean the satellite operators and data providers and distributors would be obliged to consult with particular data subjects identifiable on their satellite data, and obtain their consent to whatever use of such data would be made.

So far, perhaps commercially available satellite data may not likely be able to provide 'pictures' allowing for the individual identification of particular data subjects as such, but the scope of the protection concerns *any* information directly referring to an individually identified or identifiable person – so this may include homes and backyards of people, or company compounds wherever the applicability of privacy regulation under the European Convention on Human Rights is taken into consideration.

The precise extent and implementation in practice of applicable exceptions such as regarding public and state security, defence, and state activities in areas of criminal law may thus become crucially relevant regarding the viability of such activities in the European context[214], where it is again to be noted that so far little if any EU-wide harmonisation exists – simply because it so far fall outside the scope of competences of the Union, and under the principle of 'subsidiarity'[215] requires a distinct transfer of the competences to legislate on these issues from the sovereign member states to the Union.

3.3.4 Concluding Remarks

Even if limiting the analysis, as is the case here, to the two contexts of the European Convention on Human Rights and EU law, and foregoing discussion of the extent to which ESA and EUMETSAT in their contractual dealings with data users and consumers may have addressed the issue of privacy, it is clear that there is no single, unified European approach on handling such privacy questions in the context of VHR satellite data.

The approaches under either legal framework are already different in territorial scope, with the partisanship to the European Convention on Human Rights extending considerable beyond the member states of the European Union. Then, all member states of the latter may also be amongst the former and also the European Union itself and its individual institutions as such are bound by the European Convention, but this does not preclude divergent implementation and findings in equivalent cases. In the one case the European Convention would be applied and in another the Data Protection Directive; or the European Convention would be applied in the one case by the European Court of Human Rights (in Strasbourg) and in another by the Court of the European Union (in Luxembourg) – not to mention the possible involvement of various national courts; the result is legal and procedural complexity and uncertainty.

With a view to such possible divergences, the different phrasings of 'privacy' and 'personal data' as the respective key concepts already reflect a fundamental difference in approach. As said, the Data Protection Directive and follow-on EU law is essentially interested in *equivalent* levels of protection of personal data as a key item in economic activities, not necessarily as such in a high or low level of protection, following a desire to achieve a balance of any level of protection with free trade concerns, whereas the European Convention and follow-on jurisprudence take the human rights aspect of any interference with privacy as the supreme yardstick against which to measure any discussions on protection thereof.

Certainly, GMES will spur further discussions on whether these divergences (not to mention the contractual arrangements of ESA and EUMETSAT as relevant, once added to that discussion) may require a more specific and dedicated regime to deal with potential interference of privacy by VHR satellite data at least within the European Union, in particular where downstream involvement of the private sector in data distribution and usage of GMES data would become reality. Certainly from a European perspective, achieving a larger measure of clarity and harmonisation would greatly contribute both to the benefits VHR remote sensing data and such programmes as GMES may bring and to the preclusion of unwanted and unnecessary interference of privacy as a fundamental human right by such activities – thus further legitimising European VHR remote sensing operations and GMES.

sors established in third countries, under Directive 95/46/EC, of 27 December 2001; OJ L 6/52 (2002).

[213] Gaudrat, Tuinder, 354; Macrory, Purdy: 84-86.

[214] Purdy, 71-74.

[215] Art. 5, Treaty on European Union as amended by the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007; OJ C 306/1

4. Roundtable Discussion and General Conclusions

The following is a summary of the roundtable discussions that followed the presentations of the invited experts. The conference was closed by a roundtable discussion moderated by Rainer Sandau and Kai-Uwe Schrogl where participants, George Cho, Tanja Masson-Zwaan, Ray Purdy and Gunter Schreier elaborated further on key issues raised during the presentations of the previous sessions. On that basis a chart was presented to the speakers and the audience as guidance for the discussions marking five main areas for discussion:

The discussion ran along five main themes:

- The efficient use of EO data for treaty verification
- The improved use of EO data for law enforcement
- The effective use of EO data in disaster management
- Maintenance of privacy in using EO data
- The European dimension and the need for action

The debate kicked off with discussion of the use of EO data for treaty verification. During the presentations in the previous sessions it had been observed that the use of appropriate data, as well as the avoidance of misuse of that data, are essential to reliable treaty verification. Given the reliability of EO data, its value for treaty verification is uncontested, however, the use of this kind of data for treaty verification is not compulsory and it is not incorporated in treaties. The incorporation of this kind of data in the wording of international treaties is part of current discussions. During the conference discussions it was argued that the incorporation of the use of EO data as a measure for treaty verification would contribute to reinforce the binding nature of treaties. However, it was also pointed out that the use of EO data for treaty verification already occurs on a voluntary basis and without freezing the use of this type of data by incorporating this practice in treaties.

Moving on to law enforcement, the challenges found in this area are also related to the appropriateness of data and the correct use of it. The use of EO data for law enforcement faces on the one hand, the lack of knowledge of the potential uses of EO data and on the other hand, the lack of training for the correct interpretation and use of such data. In this sense, it was pointed out that EO data can be used by the most commonly known law enforcement authorities such as judges and police but also by other actors in charge of implementing the law, such as attorneys, local administrators in charge of the implementation of local rules or insurers. Law enforcement may also be distorted by the misuse or discarding of EO data when the law enforcer is not able to identify the value of the EO data. It was argued that action is needed at two levels for ensuring the effective use of EO data. On the one hand, awareness raising activities are needed in order to broaden the use of EO data for the maximum benefit of law enforcement activities and, on the other, capacity building activities must be promoted in order to ensure that EO data is used properly.

The question of privacy and open access to EO data was also discussed together with the open access to data for law enforcement purposes. It is widely accepted that public authorities must be able to access EO data on an open basis for the development of public services. In this regard the role of the GMES open services was highlighted for the support of law enforcement activities. However, it was also stated that national security and sovereignty matters still remain a concern that limits access to data, including by public authorities. In the case of GMES, data provided by the GMES open service will be available for use in law enforcement in the area of environment, whereas restrictions will be applicable to security in the GMES security core service.

The use of the EO data for disaster management is dominated by the application of the Disasters Charter, which is based on the agreement between different space agencies to share EO data for supporting aid and rescue management in the event of natural disasters. Although the Charter is not an international treaty, it is designed for space agencies to share EO data to assist affected countries. In view of the obstacles deriving from the lack of capacity of such countries to manage EO data in crisis situations, or even their

unwillingness to use the provided data or have them openly available, the possibility of converting the Charter into a treaty was raised as a measure to oblige the use of EO data in the aftermath of natural disasters. However, this position did not find much backing among the participants as the Charter is already working satisfactorily; in addition, the possibility of a treaty seemed very unlikely.

Privacy issues were also considered during the debate. If during the presentations it was made clear that there is no unique conception of privacy but different ways of interpreting it according to the social community and the moment in history, the debate tried to shed some light on how to attain a minimum common denominator for privacy while making it compatible with geospatial data. The specificity of space was also considered for the elaboration of a concept of privacy suitable to the utilisation of EO data. Finally, the common understanding was that privacy issues arising from the use of data are common to all areas regardless of the specificities of any area. It was also argued that space law is a grouping of different disciplines of law. As a consequence, general legislation on the preservation of privacy applies to geospatial data as it does to other areas such as telecommunications. It was felt that there is no need to bring privacy considerations explicitly into space law. However, market considerations of open access as well as interoperability with other types of data pose certain challenges regarding the ownership of and responsibility for such data. Technical characteristics also need to accommodate those challenges. Therefore it was considered that the creation of regulatory instruments containing privacy related safeguards would be useful for the avoidance of privacy issues connected to technical specificities.

The debate ended with a discussion of potential European action. Leaving aside considerations on the concept of privacy, the attention of the discussion focused on the convenience of a European quality seal for EO data. It was agreed that a European quality seal for EO data would ensure the reliability of geospatial data for verification and law enforcement. For the sake of efficiency, certification should be flexible, based on simple procedures that can easily be transferred from case to case, and higher regulatory levels such as EU secondary legislation should be avoided.

All in all, the roundtable highlighted the main concerns related to the topics that had been discussed during the sessions, bringing together the views of experts from the legal and engineering fields, while providing ideas and views on how to address them.

Matxalen Sánchez Aranzamendi
ESPI Resident Fellow

Rainer Sandau
Chairman ISPRS-IPAC

Kai-Uwe Schrogl
Director ESPI

European Space Policy Institute

ISPRS/ESPI/IAA/IISL Conference - Current legal issues for satellite Earth observation

Topics with related issues and problems

1. Efficient use of EO data for treaty verification
- Do we have the right data?
- How to get to provisions using EO data for treaty verification wherever technically feasible? (are there any areas, where special effort to introduce it should be undertaken?)
- How to avoid misuse and false information?
- How to bring space law and other relevant "terrestrial" law together? How to come to harmonized provisions?

2. Improved use of EO data in law enforcement
- Do we have the right data?
- How to ensure confidence in and reliability of data?
- How to shape definitions for the use (in particular related to privacy)? What can other countries derive from the U.S. experience?
- How to better communicate and promote the use in court?

3. Effective use of EO data in disaster management
- Do we have the right data? Is the integrated use of EO, telecom and positioning working well?
- Is there a need to make the Charter a binding legal instrument and extend its scope? (might this help to dealing with governments, which do not want to receive help, or where no government is functioning?)
- Should there be comparable arrangements like the Charter for the use of other satellite applications?

4. Maintenance of privacy in using EO data
- How to attain a minimum common denominator for privacy? Are international principles achievable? How to make this minimum coherent with the tech capacities in the field of geospatial data.
- Is self regulation a solution?
- How to draw the balance between private and public interest?
- Do we need specific legal provisions in space law regarding privacy or are general existing provisions sufficient?
- With reference to 2.: how to balance privacy and better law enforcement?

5. European dimension and need for action
- How to shape GMES missions (ESA, Eumetsat, national) to serve treaty monitoring, law enforcement and disaster management?
-How to define the roles in the setting of regulations based on the Lisbon Treaty (new roles of the actors, in particular EU institutions; provisions other than the space competence)?
- Define a European quality seal for EO data to be used in court?

www.espi.or.at

List of Acronyms

A	
ABC	Australian Broadcasting Corporation
ADRC	Asian Disaster Reduction Centre
AU	Authorized User
B	
BNSC	British National Space Centre
C	
CCTV	Case of Closed-Circuit Television
CNES	Centre National d'Etudes Spatiales
CNIL	National Commission for Infromatics and Freedoms
CNSA	China National Space Administration
CONAE	Comisión Nacional de Actividades Espaciales
CSA	Canadian Space Agency
CTBT	Comprehensive Nuclear-Test-Ban Treaty
CWC	Chemical Weapons Convention
D	
DMC	Disaster Monitoring Constellation
DEM	Digital Elevation Model
E	
EC	European Community
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
EO	Earth Observation
ESA	European Space Agency
ERTS	Earth Resources Technology Satellite
ESPI	European Space Policy Institute
EU	European Union
EMSA	European Maritime Safety Agency
F	
FRE	Federal Rules of Evidence
FP7	7th Framework Program
G	
GEO	Group on Earth Observation
GEOSS	Group on Earth Observation System of Systems
GII	Global Information Infrastructure
GIS	Geographic Information Systems
GMES	Global Monitoring for Environment and Security
GNSS	Global Navigation Satellites System
GPS	Global Positioning System
GSC	GMES Space Component
GSD	Ground Sample Distances
I	
IAEA	International Atomic Energy Agency
ICCPR	International Covenant on Civil and Political Rights
ISRO	Indian Space Research Organisation
IT	Information Technology

ITS	Intelligence transport system
L	
LIMES	Land and Sea Integrated Monitoring for European Security
LCT	Laser Communication Terminal
LTBT	Limited Test Ban Treaty
M	
MINUSTAH	United Nations Stabilisation Mission in Haiti
N	
NOAA	National Oceanic and Atmospheric Administration
NTM	National Technical Means
NZ	New Zealand Bill of Rights Act
O	
OLCI	Ocean Land Color Instruments
P	
PIT	Privacy-Invasive Technologies
PPP	Public Private Partnership
PRS	Public Regulated Service
PST	Privacy-Sympathetic Tools
S	
SVCs	Stored Value Cards
SSO	Sun Synchronus Orbit
U	
UNDHR	Universal Declaration of Human Rights
UNCOPUOS	United Nations Committee on Peaceful Uses of Outer Space
UNEP	United Nations Environment Program
UNISPACE	United Nations Conference on the Exploration and Peaceful uses of outer space
UNITAR	United Nations Institute for Training and Research
UNOOSA	United Nations Office for Outer Space Affairs
UNOSAT	UNITAR Operational Satellite Applications Programme
USGS	United States Geological Survey

Workshop Programme

Satellite Earth observation is becoming more and more an efficient tool for monitoring all kinds of resources of Earth. Remotely sensed data are now a reliable basis for decision-making in many areas of society. We experience increasing resolutions both spatially and spectrally. Constellations of small satellites are capable to provide good daily coverage of the Earth's surface and allow to increase the temporal resolution. The progress resulting from satellite Earth observation allows to expand the application fields but also brings to light new problems to be discussed in a broader public debate.

This Conference deals with two important and topical aspects of satellite Earth observation:
- treaty monitoring and law enforcement through satellite Earth observation,
- privacy conflicts from high resolution imagery.

It brings together experts from the remote sensing and in the legal fields. It i.a. aims at decision-makers in the field of treaty monitoring and international law enforcement (foreign and environment ministries, international organizations). This provides the unique opportunity to discuss the different implications stemming from the technology developments and applications as well as from legal and regulatory perspectives.

The focus of the discussions at this Conference is to optimise the regulatory framework for satellite Earth observation thus supporting the full implementation of its potentials.

Venue:

ESPI
Palais Fanto
Schwarzenbergplatz 6
(Entrance: Zaunergasse 1-3)
A-1030 Vienna, Austria
Tel +43 1 718 1118 -0 / Fax -99
www.espi.or.at

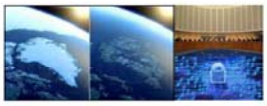
Registration fee: 150 €

Registration: office@espi.or.at

ISPRS/ESPI/IAA/IISL Conference

Current legal issues for satellite Earth observation

Programme



ESPI
Vienna, Austria
8-9 April 2010

Thursday, 8 April 2010

14:00-14:15 Welcome

Kai-Uwe Schrogl, Director ESPI
Tanja Masson-Zwaan, President IISL
Jean-Michel Contant, Secretary General IAA

14:15-14:30 Introduction

Rainer Sandau, Chairman ISPRS-IPAC

14:30-18:00 Session 1

Treaty monitoring and law enforcement through satellite Earth observation

Moderator: Sa'id Mosteshar

14:30-15:15 Overview on legal issues
Ray Purdy
Deputy Director of the Centre for Law and the Environment
Faculty of Laws, University College London
Bentham House

15:15-16:00 What's in GMES for treaty monitoring and law enforcement
Gunter Schreier
GMES Coordinator
German Aerospace Center DLR, Oberpfaffenhofen

16:00-16:45 **Moved from session 2**
Google's Earth Observation interests
Ed Parsons
Geospatial Technologist
Google, London

16:45-17:15 Coffee break

Moderator: Matxalen Sánchez Aranzamendi

17:15-18:00 The Charter on Space and Major Disasters
Atsuyo Ito
Researcher, Tokyo

18:00-18:45 Use of satellite data for treaty monitoring
Jana Jentzsch
Attorney-at-law, Hamburg

18:45-19:30 Use of satellite data for law enforcement
Jean-Francois Mayence
Legal Affairs and International Relations
Belgian Federal Office for Science Policy
Lector Katholieke Universiteit Leuven

19:30 Reception

Friday, 9 April 2010

09:00-12:30 Session 2

Privacy conflicts from high resolution imaging

Moderator: Frans von der Dunk

09:00-09:45 Overview on legal issues
George Cho
Chair, Academic Board, Professor of Geoinformatics and the Law
Faculty of Applied Science, University of Canberra

09:45-10:30 What is "privacy"? Perceptions around the world
Catherine Doldirina
Institute of Air and Space Law
McGill University, Montréal

10:30-11:15 The European Convention on Human Rights and EC law - 'Two European legal approaches to privacy, as relevant to high-resolution imaging
Frans von der Dunk
Harvey and Susan Perlman Alumni/Othmer Professor of Space Law
Space and Telecommunications Law Program
University of Nebraska-Lincoln, College of Law

11:15-11:45 Coffee break

11:45-13:00 Roundtable

Moderators: Rainer Sandau and Kai-Uwe Schrogl
Participants: George Cho, Tanja Masson-Zwaan, Ray Purdy and Gunter Schreier

13:00 Closing and buffet lunch

About the Contributors

Orhan Altan

Orhan Altan is ISPRS President. He graduated in Civil Engineering at Istanbul Technical University. In 1970 he joined the Chair of Photogrammetry, where he finished his PhD in 1974. In 1989 he became full Professor at the University.Since 1989 He is the Head of the Division of Photogrammetry at the Technical University of Istanbul. He is member of many national and international organisations and acted since 2004 as the Secretary General of ISPRS.

George Cho

George Cho is Chair of Academic Board and Professor of Geoinformatics and the Law at the University of Canberra, Australia. He is a research scientist with the Institute for Applied Ecology and is the Head of School, Resource, Environmental and Heritage Sciences. His research focuses on the study of the legal and policy issues affecting geographic information science and the practical problems in the application of technology in the creation, use and impact of digital spatial information. He teaches courses in geographic information systems, environmental law, electronic law for business and government especially e-business and e-commerce and international trade, intellectual property law and the law of cyberspace.

Dr. Cho has held academic teaching and research appointments at various universities including as Research Scholar at the Australian National University, Canberra; Tutor and Lecturer at the University of Malaya, Kuala Lumpur; Teaching Assistant at the University of British Columbia, and Visiting Lecturer at Liverpool, England, Maynooth College, National University of Ireland, University of Hanoi, Keele University, England and the University of Canterbury, NZ.

Prof. Cho has published numerous books and journal articles on law and geography topics, including *Contracts: Australia. International Encyclopaedia of Laws (*with E Clark, Griggs, L and A Hoyle), The Hague: Kluwer Law International 2010; *Geographic Information Science: Managing the Legal Issues* (London: John Wiley & Sons, 2005); *Cyber Law: Australia. International Encyclopaedia*

Catherine Doldirina

Catherine Doldirina is a PhD candidate at the Institute of Air and Space Law, McGill University. She has been conducting legal research relating to space activities since 2005. Her expertise lies in the field of intellectual property law and her current research relates to the legal status of remote sensing data. She has lectured on European competition law, European copyright law and space law at the University of Bremen and at the European Humanities University (Lithuania). She has also tutored at the European Centre for Space Law summer school on space law and policy. Her professional experience was gained as legal assistant to specialist copyright lawyers (Bremen). She successfully completed an internship at the European Space Policy Institute, Vienna, drafting the study “Case for Space” during this time. She authors work on other aspects of space law, is engaged in the research activities at the Institute of Air and Space Law, as for example Space Security Index, and is a member of the International Institute of Space Law. In 2009 she was awarded the Diderick Verschoor award and prize for the best paper by a young author for the Colloquium on Space Law of the International Institute of Space Law.

Frans G. von der Dunk

Frans G. von de Dunk holds the Harvey and Susan Perlman Alumni / Othmer Chair of Space Law at the University of Nebraska-Lincoln’s LL.M. Programme on Space and Telecommunication Law (for more information on the programme: see http://law.unl.edu/spacelaw) since January 2008. He also is Director of Black Holes BV, Consultancy in space law and policy, based in Leiden (for more information: see http://www.black-holes.eu). Previously, he was Co-Director, then Director of Space Law Research at the International Institute of Air and Space Law at Leiden University since 1990.

Prof. Von der Dunk was awarded the Distinguished Service Award of the International Institute of Space Law (IISL) of the International Astronautical Federation (IAF) in Vancouver, in October 2004, and the Social Sci-

ence Award of the International Academy of Astronautics (IAA) in Valencia, in October 2006. In the summer of 2008, he was nominated, as the first lawyer ever, Member of the European Space Sciences Committee (ESSC) of the European Space Foundation (ESF). Also, he was the sole lawyer on the Panel on Asteroid Threat Mitigation established by the Association of Space Explorers (ASE) in 2007.

He defended his dissertation on "Private Enterprise and Public Interest in the European 'Spacescape'" in 1998. He has written well over 120 articles and published papers, has given more than 100 presentations at international meetings and was visiting professor at some 25 foreign universities across the world on subjects of international and national space law and policy, international air law and public international law. He has (co-)organised some 20 international symposia, workshops and other events, and has been (co-)editor of a number of publications and proceedings. As of 2006, he is the Series Editor of 'Studies in Space Law', published by Brill. In addition, he has given a range of interviews to the international media on issues of space law and policy.

Prof. Von der Dunk has served as adviser to the Dutch Government, several foreign Governments, the European Commission, the European Space Agency (ESA), the United Nations (UN), the Organisation for Economic Co-operation and Development (OECD), the Dutch National Aerospace Agency (NIVR), the Japanese Space Exploration Agency (JAXA), the German Space Agency (DLR), the Brazilian Space Agency (AEB), the Swedish Space Corporation (SSC) and the Centre for Strategic and International Studies (CSIS), as well as a number of companies. Such advisory work dealt with a broad area of issues related to space activities, such as space policy, international cooperation in space, national space law, privatisation of space activities, Global Navigation Satellite Systems (GNSS) (in particular Galileo), satellite communications, radio astronomy, and earth observation. Also, he has acted as the Legal Task Manager in a number of studies undertaken in particular within the context of leading European Commission projects, such as on European space policy, Galileo and GNSS, satellite communications, the Global Monitoring for the Environment and Security (GMES) project and earth observation. Much of his recent work furthermore focused on such topical issues as space tourism, the legal status of the Moon and other celestial bodies and the 'sale-of- lunar-estate hoax', and planetary protection.

He is Director Public Relations of the International Institute of Space Law (IISL), Member of the Board of the European Centre for Space Law (ECSL), and Member for the Netherlands in the International Law Association's (ILA) Committee on Space Law. He is also Member of the International Editorial Board of 'Space Policy'. Further memberships include: International Academy of Astronautics (IAA), American Branch of the International Law Association (ABILA), International Bar Association's (IBA) Section on Business Law (SBL), Committee Z on Outer Space Law, International Policy Advisory Committee (IPAC) of the International Society of Photogrammetry and Remote Sensing (ISPRS), American Institute of Aeronautics and Astronautics (AIAA; Senior Member), and Centro de Investigacion y Difusion Aeronautico-Espacial (CIDA-E; Corresponding Member).

Atsuyo Ito

Atsuyo Ito is a research fellow at Social Science Research Institute, International Christian University, Tokyo, Japan. She holds a Ph.D degree in law from University of Paris XI, and LL.M in international air and space law from Leiden University, the Netherlands. Dr Ito has worked for the Remote Sensing Unit, Science Sector of UNESCO and has recently undertaken a research project for the Ministry of Economy, Trade and Industry (METI) of the Japanese Government. In 2004, she received the Prof. Dr I.H.Ph. Diederiks-Verschoor Award and has written numerous articles and papers in the field of space law, satellite remote sensing, as well as disaster management.

Tanja Masson-Zwaan

Tanja Masson-Zwaan is Deputy Director, International Institute of Air and Space Law, Leiden University, The Netherlands and the President of the International Institute for Space Law.

She has specialised in the field of air and space law since 25 years. She currently teaches air and space law in the advanced Masters programme (LLM) in air and space law of Leiden University, and carries out various research activities. She is the President of the International Institute of Space Law and has published papers on a variety of topics over the years. She lectures on space law all over the world, advises the Dutch government and other national and international bodies on matters relating to space law, and attends the sessions of the United Nations Committee on the Peaceful Uses of Outer Space as an observer.

Before returning to Leiden where she graduated in international law, she set up and taught courses in air and space law at the National University of Singapore, worked as a consultant in France and the Netherlands for industrial and institutional clients, and served many years as Executive Secretary of the IISL.

Tanja is a recipient of several awards and is a member of various professional organisations such as the International Astronautical Academy (IAA), the Académie de l'air et de l'espace (ANAE, France), the International Law Association (ILA), the European Centre for Space Law (ECSL), the International Aviation Women's Association (IAWA), and a Board member of Women in Aerospace-Europe and the Netherlands Society for Aerospace (NVR).

Jean-François Mayence

Jean-François Mayence is the Head of the Legal Unit "International Relations" at the Belgian Federal Office for Science Policy. He is in charge of legal aspects of international cooperation programme in various fields, including space research & applications, but also Antarctica, generic sciences, human sciences, etc. In that capacity, he was member of the Belgian Delegation to ESA during 9 years and I'm member of the Belgian Delegation to UNCOPUOS since 1999. I'm also lector at University of Leuven, teaching legal aspects of space activities.

Ray Purdy

Ray Purdy joined the law faculty in 2000 and is a senior research fellow and deputy director of the University College London Law faculty's centre for law and the environment. He had previously held academic positions as a researcher at Imperial College and the University of Oxford, as well as a visiting lectureship at City University.

His most recent research has focused on the use of satellite remote sensing to monitor and enforce laws. Ray is particularly interested in environmental law applications for satellites, how they might influence regulatory compliance, and evidential and privacy implications. Between October 2005 and December 2008 he was funded on a 3.25 year contract as project manager and lead researcher on an Arts and Humanities Research Council funded programme on satellite monitoring as a legal compliance tool in the environmental sector. From April 2009, Ray is PI on an 18-month ESRC Research Grant entitled 'Smart Enforcement in Environmental Legal Systems: A Socio-Legal Analysis of Regulatory Satellite Monitoring in Australia'.

Matxalen Sánchez Aranzamendi

Matxalen Sánchez Aranzamendi is Resident Fellow at the European Space Policy Institute (ESPI) in Vienna, Austria since 2008. She has specialised in European Integration and owns an Advanced LLM in European Business Law. Before joining ESPI she had dealt with EC Space Policy and GMES issues during her internship at the European Commission and previously she had been a Junior Policy Advisor for the Delegation of the Basque Country in Brussels where she dealt with EC Transport Policy and Galileo affairs. Currently she focuses on national space legislations and space related regulations.

Rainer Sandau

Rainer Sandau is retired from the German Aerospace Center (DLR) after over 30 years of experience in space activities. He was involved in instrumentations of space missions to Venus, Mars and Earth, and also in numerous concepts for instruments and small satellites for or with different countries and space agencies, e.g. Argentina, UK, Russia, Taiwan, Tunisia, CNES, ESA, NASA, ranging from the concept of a German stereo camera on-board the French SPOT 5 mission to a lander concept jointly done with NASA/JPL for ESA's cometary mission ROSETTA. During his career he held different positions, including Deputy Director of the Institute of Space Research in East-Berlin after the wall came down, and Director R&D of the Swiss/US company LH Systems based in Switzerland (Leica Company). He is member of various national and international associations, for instance member of the International Academy of Astronautics (IAA) where he serves as Technical Director Satellites and Space Applications, and chair of the International Policy Advisory Committee (IPAC) of the International Society of Photogrammetry and Remote Sensing (ISPRS). As IPAC chair, he is the ISPRS representative to the Committee on Peaceful Uses of Outer Space within the United Nations' General Assembly (UN COPUOS). He authored or co-authored over 250 publications, holds over 30 patents, is member of the Editorial Advisory Boards of the ISPRS Journal of Photogrammetry and Remote Sensing, and is editor or co-editor of 19 books or conference proceedings, all dealing with the topics small satellite missions, remote sensing and photogrammetry.

Gunter Schreier

Gunter Schreier is working as Head of Business Development at the German Remote Sensing Data Center of DLR (DLR-DFD) and is the coordinator for GMES related projects.

He has served at DLR in several functions since 1985, among others as Head of the Technology Transfer unit and team leader for establishing the ESA-ERS „Processing and Archiving Center“. He has business experience as founding Vice President Geomatics for Definiens and has worked as national expert at the Joint Research Center of the European Commission. He has contributed to Earth Observation standards and data policy in several international groups such as CEOS, IGBP-DIS, UNEP and ISPRS and is member of the ISPRS International Policy Advisory Group and the IAF Earth Observation Committee. Gunter Schreier has a diploma in Geophysics from University of Munich.

Kai-Uwe Schrogl

Kai-Uwe Schrogl is the Director of the European Space Policy Institute (ESPI) in Vienna, Austria since 2007. Before, he was Head of Corporate Development and External Relations Department in the German Aerospace Center (DLR). In his previous career he worked with the German Ministry for Post and Telecommunications and the German Space Agency (DARA). He has been delegate to numerous international forums and recently served as the chairman of various European and global committees (ESA International Relations Committee, UNCOPUOS working groups). Kai-Uwe Schrogl has published nine books and more than 100 articles, reports and papers in the fields of space policy and law as well as telecommunications policy. He is editor of the “Yearbook on Space Policy” and the book series “Studies in Space Policy” both published at SpringerWienNewYork as well as member in editorial boards of international journals in the field of space policy and law (Acta Astronautica, Space Policy, Zeitschrift für Luft- und Weltraumrecht, Studies in Space Law/Nijhoff). Kai-Uwe Schrogl is Member of the Board of Directors of the International Institute of Space Law, Member of the International Academy of Astronautics (chairing its Commission on policy, economics and law) and the Russian Academy for Cosmonautics. He holds a doctorate degree in political science, lectures international relations at Tübingen University, Germany (as a Honorarprofessor) and has been a regular guest lecturer i.a. at the International Space University and the Summer Courses of the European Centre for Space Law.

Speakers at the conference (from left): Kai-Uwe Schrogl (ESPI), Ray Purdy (Faculty of Laws, University College London Bentham House), Catherine Doldirina (McGill University, Montreal), Jean-Michel Contant (IAA), Matxalen Sánchez Aranzamendi (ESPI), Gunter Schreier (DLR), Ed Parsons (Google Earth), Herbert Allgeier (Chairman of the ESPI Advisory Council), George Cho (Law Faculty of Applied Science, University of Canberra), Frans G. von der Dunk (Space and Telecommunications Law Program, University of Nebraska), Sai'd Mosteshar (London Institute for Space Policy and Law), Atsuyo Ito (Researcher, Tokyo), Rainer Sandau (ISPRS-IPAC), Jean-Francois Mayence (Belgian Federal Office for Science Policy), Tanja Masson-Zwaan (IISL), Jana Jentzsch (Attorney-at -law, Hamburg)

Mission Statement of ESPI

The mission of the European Space Policy Institute (ESPI) is to provide decision-makers with an independent view and analysis on mid- to long-term issues relevant to the use of space.

Through its activities, ESPI contributes to facilitate the decision-making process, increases awareness of space technologies and applications with the user communities, opinion leaders and the public at large, and supports researchers and students in their space-related work.

To fulfil these objectives, the Institute supports a network of experts and centres of excellence working with ESPI in-house analysts.

www.espi.or.at