1-1-2009

Europe and the 'Resolution Revolution': 'European' Legal Approaches to Privacy and Their Relevance for Space Remote Sensing Activities

Frans G. von der Dunk
University of Nebraska - Lincoln, fvonderdunk2@unl.edu

Published in the Annals of Air and Space Law (2009) 34.

EUROPE AND THE 'RESOLUTION REVOLUTION':

'EUROPEAN' LEGAL APPROACHES TO PRIVACY AND THEIR RELEVANCE FOR SPACE REMOTE SENSING ACTIVITIES

by

Frans G. von der Dunk*

SYNOPSIS

* Professor of Space Law, Lincoln, College of Law, University of Nebraska. He is also Director of the recently established Black Holes BV, Consultancy in space law and policy, based in Leiden. Prior to the foregoing, he held the positions of Co-Director, and subsequently Director of Space Law Research at the International Institute of Air and Space Law at Leiden University since 1990.

ABSTRACT

With the increasing general availability of very high resolution (VHR) satellite remote sensing data, issues of potential invasion of personal spheres of privacy will become ever more important. As of yet, there is no international law providing for a clear-cut regime balancing the freedom of information, including information gathering, with the rights of individual persons to remain free from interference with their privacy. The latter issues therefore essentially can be tackled only at a national level, with the obvious disadvantage that any regulation remains principally limited in scope to the national jurisdiction concerned.

Also at the European level this essentially holds true, although two separate developments are making considerable inroads into this situation. On the one hand, by means of the European Convention on Human Rights, which does recognize a human right to privacy, an overarching regime has been created that largely limits individual member states of the Council of Europe in their discretion to deal with that right as they see fit.

On the other hand, from a perspective of prevention of undue distortion of the Internal Market through major variations in the extent to which (the application of) privacy laws might result in obstacles to the free flow of information within the European Union, a body of EC law is evolving which harmonizes the applicable laws to a considerable extent.

This paper analyzes both developments, and represents an effort to relate them to each other with a view in particular as to how they might impact satellite remote sensing operations, once these would actually come to be seen as infringing personal privacy. Its final conclusion is that, indeed, the combination of those two European legal approaches to privacy leads to a sensible compromise on handling the potential effects on privacy flowing from the 'resolution revolution' in satellite remote sensing data.

RÉSUMÉ

La disponibilité accrue de données télédétection très haute résolution renforce le problème de l'empiètement sur le droit à la vie privée. Jusqu'a maintenant, aucune loi internationale n'avait établi de distinction juridique permettant de mettre en balance les intérêts concurrents de la liberté de l'accès à l'information et de la collecte d'informations avec le droit de l'individu au respect de sa vie privée. Par conséquent, les tribunaux devront trouver des solutions aux problèmes juridiques en droit domestique, avec pour inconvénient majeur, un champ d'application restreint à celui de la loi étatique.

Ce problème existe en Europe comme ailleurs, mais la situation tend quelque peu à s'éclaircir grâce à deux tendances. Premièrement la Convention européenne des droits de l'homme reconnaît le droit à la vie privée, et le régime obligatoire de cette Convention limite considérablement la marge de manœuvre des États Membres du Conseil de l'Europe dans leur interprétation de ce droit. Deuxièmement, afin d'éviter la distorsion du marché interne qui pourrait résulter de l'application de différentes lois domestiques sur l'accès à l'information, le droit européen est en train d'harmoniser considérablement les règles applicables.

Cet article analyse ces deux développements et tente de discerner la relation entre eux, surtout pour déterminer l'effet sur les opérations de télédétection par satellite lorsqu'il est établi que ces opérations empiètent sur le droit à la vie privée. La conclusion de l'article est que ces deux approches juridiques européennes représentent un compromis intéressant pour les effets potentiels sur la vie privée des données télédétection très haute résolution.

I. SPACE REMOTE SENSING, PRIVACY PROTECTION ISSUES AND THE EUROPEAN CONTEXT

One of the most important recent global developments in space activity is that triggered by the increasing generation of very high resolution (VHR) satellite remote sensing data. Its worldwide availability, driven by Google Earth and its equivalents (for obvious commercial reasons) making crucial use of modern telecommunication infrastructure such as the Internet, helps to spur on a revolution in satellite imagery and data acquisition. These developments manifest themselves in the rapidly increasing possibilities now available to individuals to, potentially, monitor and intrude in on other individuals' private lives, and the concurrent growing interest of commerce in such potential.

Personally, I received a forewarning of the potential impact of such developments a number of years ago when a German businessman approached me with his idea to offer certain mementoes for sale to tourists leaving the peninsula of Mount Athos, a religious enclave within Greece. The mementoes in question concerned satellite pictures of the peninsula and its monasteries. He was, however, faced with a refusal by the Greek authorities to permit him to sell such mementoes near the 'exit' of Mount Athos since the intrusion upon the prevailing religious atmosphere as per these 'satellite close-ups' was considered unacceptable. He wondered whether such a prohibition was not in violation of the freedom of space activities, in particular remote sensing, as he understood it to be enshrined within the Outer Space Treaty[1] and international law.[2]

---

[1] See *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* (hereafter Outer Space Treaty), 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), in particular Art. I which states amongst other things: "Outer space, including the Moon and other celestial bodies, shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law".

[2] In regard of remote sensing, the freedom of using outer space within the limits of

The answer, of course, was both yes: the freedom of remote sensing prevented the Greek government from prohibiting the *generation* of those satellite pictures of Mount Athos (at least under international law – in other words, as long as the relevant operator was not Greek or operating from Greek territory); and no: there was nothing legally incorrect with the prohibition imposed by the Greek authorities on the *distribution* such data within Greece, as this was comprehensively subsumed under the sovereignty of Greece. As such, Sovereign competencies would certainly extend to any efforts to preserve the virtual integrity of the monasteries in terms of such intrusion, and to consider such rights to virtual integrity more important than relevant business interests.

It therefore seems that while international law positively stimulates the worldwide flow of information and data as freely as possible, national law is then often called upon to try and preserve the interests of individual people or entities to have information and data pertaining to them less freely circulated. This dichotomy could only rise to pre-eminence with the 'resolution revolution', since this revolution, for the first time, spawned data of such high resolution that privacy can become fundamentally challenged in the process. In the above instance, the privacy was of a larger-than-individual nature - but the next step to intrusion in personal privacy is only a small one.[3]

As revolutions are wont to do, this one has to some extent started to eat its own children. The CEO of Google Earth was not very pleased, to put it mildly, when he found his mansion including swimming pool and other edifices to be easily and rapidly pointed out on the Internet, using Google data. Recently, whether as a consequence of this 'event' or not, Google Earth announced its general interest in cooperating with relevant authorities to ensure that a correct balance would be struck between privacy concerns and any commercial interests involved. This expression of interest was clarified as being acceptable only with the

---

international law has taken on the particular shape of freedom of information-gathering from space and the distribution of such data. This freedom is only marginally limited by the provision of Principle XII of the *Principles Relating to Remote Sensing of the Earth from Outer Space* (hereafter Resolution 41/65), UNGA Res. 41/65, of 3 December 1986; UN Doc. A/AC.105/572/Rev.1, at 43; 25 ILM 1334 (1986); that "As soon as the primary data and the processed data concerning the territory under its jurisdiction are produced, the sensed State shall have access to them on a non-discriminatory basis and on reasonable cost terms".

[3] See e.g. R. Purdy, 'Satellites: A New Era for Environmental Compliance', (2006) 3:5 Journal for European Environmental and Planning Law, 407-8; 412-3.

least possible interference with opportunities to generate, distribute and use relevant data.

Regardless of these Google Earth-centered events, it will be clear that the underlying developments in this area do draw issues of the protection of privacy of individuals into the picture. This paper addresses the issue from a particular European vantage point because, in Europe, the dichotomy between international law and national law is to some extent bridged by legal developments at an intermediate level.

In this respect, it is important to note that when it comes to 'European legal approaches' to privacy protection in law, and their potential or actual impact upon space-based remote sensing activities, one should look elsewhere than space lawyers would perhaps, at first instance, be inclined to do. The 'Europe' in question is not that of the European Space Agency (ESA), as this is an intergovernmental organization created to pool the financial and technical resources of its member states for the purpose of space activities, and which does not seek to exercise any legal or regulatory control over such space activities, whether public or private.[4] Neither is it the 'Europe' of EUTELSAT[5] (even

[4] ESA was established by means of 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), which lists, in Art. II, as the primary objectives of such establishment: "to provide for and to promote, for exclusively peaceful purposes, cooperation among European States in space research and technology and their space applications, with a view to their being used for scientific purposes and for operational space applications systems, (a) by elaborating and implementing a long-term European space policy, by recommending space objectives to the Member States, and by concerting the policies of the Member States with respect to other national and international organizations and institutions; (b) by elaborating and implementing activities and programmes in the space field; (c) by coordinating the European space programme and national programmes, and by integrating the latter progressively and as completely as possible into the European space programme, in particular as regards the development of applications satellites; (d) by elaborating and implementing the industrial policy appropriate to its programme and by recommending a coherent industrial policy to the Member States".

[5] EUTELSAT was originally established as an intergovernmental organization by means of the *Convention Establishing the European Telecommunications Satellite Organization* (EUTELSAT), Paris, done 15 July 1982, entered into force 1 September 1985; Cmnd. 9069; Space Law – Basic Legal Documents, C.II.1; for the purposes of "the design, development, construction, establishment, operation and maintenance of the space segment of the European telecommunications satellite system or systems. In this context, EUTELSAT shall have as its prime objective the provision of the space segment required for international public telecommunications services in Europe" (Art. III (a)). Meanwhile, EUTELSAT operations have been commercialised, with a private operator Eutelsat being responsible for day-to-day management, operations, marketing and sales; cf. also *Convention Establishing the European Telecommunications Satellite Organization* (EUTELSAT), done 15 July 1982, entered into force 1 September 1985, as amended 20 May 1999, amended version not yet entered

before its recent privatization) as that organization essentially took over European satellite communication infrastructure; or even of EUMETSAT,[6] which did the same for satellite-based meteorology. The 'Europe' that needs to concern us here is that of, on the one hand, the Council of Europe, and, on the other hand, the European Community as it constitutes the legally relevant part of the European Union.

II. THE COUNCIL OF EUROPE AND PRIVACY: THE HUMAN RIGHTS APPROACH

The Council of Europe is one of the oldest intergovernmental organizations in Europe that sprung from the general desire to steer away from the horrors of the Second World War. It was to establish an international framework integrating several aspects of the member states' national legal orders in order to ban the nationalism and xenophobia largely considered responsible for those horrors. Its *magnum opus* was the European Convention on Human Rights,[7] serving as a catalogue of fundamental human rights to counter any tendency to permit the resurgence of such horrors.

The Council of Europe itself was established by means of the Statute of the Council of Europe, drafted in 1949.[8] Currently, it comprises 47 member states,[9] and is thus considerably broader in terms of membership than the European Union. All members of the Council of Europe as a consequence of their membership automatically became parties to the European Convention on Human Rights.

In the context of the Council of Europe, privacy has been logically

---

into force but applied provisionally 2 July 2001; Space Law – Basic Legal Documents, C.II.1.

[6] The intergovernmental organization EUMETSAT was established by means of 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 amended 14 July 1994, entered into force 27 July 1994; Cmnd. 9483; Space Law – Basic Legal Documents, C.III.1; 44 ZLW 68 (1995); in order "to establish, maintain and exploit European systems of operational meteorological satellites, taking into account as far as possible the recommendations of the World Meteorological Organization. A further objective of EUMETSAT is to contribute to the operational monitoring of the climate and the detection of global climatic changes" (Art. 2(1)).

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

[8] *Statute of the Council of Europe*, London, done 5 May 1949, entered into force 3 August 1949; ETS No. 001.

[9] See online: <http://www.coe.int/T/e/Com/about_coe>. At the time of writing, there is one applicant state as well as five observer states.

approached and is treated, first and foremost, as a (rather fundamental) human right. The principle does not attempt a balancing act between an individual interest to remain free from intrusion and other (commercial) interests in the widespread distribution and availability of personal and personalized information.

To be precise, such a legal approach was not an exclusively European one. The 1948 Universal Declaration on Human Rights,[10] drafted in the UN context for more or less the same purposes and with more or less the same approach, had included an Article 12 which prohibited any arbitrary interference with privacy and called for its protection by instruments of national (as well as international) law.[11]

The Universal Declaration was not a treaty with binding legal force, although its high political and moral status, as well as the obvious concerns for humanity behind it, caused it to be viewed by many as representing, in many respects, customary international law and, in some respects, even as *jus cogens*.[12] Most of the Declaration's principles were later elaborated upon in an international convention, the 1966 International Covenant on Civil and Political Rights. Article 17 of this Covenant, addressing the right to privacy, essentially replicates the analogous provision in the Universal Declaration.[13]

Developments in Europe, however, were considerably more rapid, as the European Convention on Human Rights was drafted as early as 1950, and was already in force in 1953. The Convention elaborated upon the succinct statement of the human right to privacy in the Universal Declaration. Article 8(1) posited the right to respect for private and family life, home and correspondence, and Article 8(2) spelt out that interference with the right to privacy by public authorities was

---

[10] *Universal Declaration of Human Rights*, Paris, UN GA Res. 217 A (III) of 10 December 1948; A/RES/217.

[11] Art. 12 of the *Universal Declaration on Human Rights*, reads in full: "No one shall be subjected 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 attacks."

[12] See Art. 53, *Vienna Convention on the Law of Treaties*, Vienna, done 23 May 1969, entered into force 27 January 1980; 1155 UNTS 331; UKTS 1980 No. 58; Cmnd. 4818; ATS 1974 No. 2; 8 ILM 679 (1969).

[13] 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); reads in full: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks."

permissible only in exceptional cases. Moreover, these exceptional circumstances ought to be clearly outlined by the relevant national law and exercised within the limits of such provisions. Such an approach was of far greater precision than the Universal Declaration.[14]

Thus, whilst Article 12 of the Universal Declaration served as a precursor to Article 8 of the European Convention on Human Rights, considerable differences exist.[15] By way of an example further to the one above, the European Convention does not expressly prohibit attacks on honor and reputation, which the Universal Declaration by contrast does. At the same time, the rights concerned are general and broad in scope, and whilst the European Convention did not seek to provide exhaustive definitions, interpretations were subsequently developed in case law, in particular in the *Pretty* case.[16]

Also, the European Convention narrows down the scope of the prohibition of interference to such interference by "public authority" only.[17] In other words: if the distribution of satellite data potentially interfering with a person's privacy is carried out by a non-governmental entity – for example a private entity acting for commercial reasons – no violation of Article 8 would arise.

Essentially, this is where a 'paparazzi-problem' arises. The right to recognition of privacy, expressed in Article 8(1) of the European Convention, applies across the board. However, the specific prohibition on interference with such privacy under Article 8(2) only applies to governmental action, a prohibition limited furthermore by specifically carved-out exceptions. In case relevant interference with privacy occurs by private action, it would ultimately be up to the judge or court of the concerned jurisdiction to decide whether the interference with the right

---

[14] The full text of Article 8 runs as follows: "(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."

[15] See further in detail J. Velu, "The European Convention on Human Rights and the Right to Respect for Private Life, the Home and Communications" in A.H. Robertson ed., *Privacy and Human Rights*, (Manchester: Manchester University Press, 1973) 14. [Velu].

[16] *Pretty v. The United Kingdom* (Application no. 2346/02, Judgment of 29 April 2002) [Pretty]; see further P. van Dijk *et al*, Eds., *Theory and Practice of the European Convention on Human Rights* 4th ed., (Oxford/Antwerpen: Intersentia, 2006) 664-5. [Van Dijk].

[17] See also *Velu*, *supra* note 15 at 17, pointing out that this limitation was a result of a British amendment to the Article, which was partially accepted.

would amount to a violation of the law. This situation might arise, for example, because there is no justification for that interference in terms of consent of the targeted individual or the violation on regulations of freedom of information gathering. The intention and focus of the European Convention is unequivocally focused on controlling impersonal governmental bureaucracies and precluding them from unfettered 'Big-Brothering', not on private or commercial intrusions.[18]

At the same time, the European Court of Human Rights has developed the concept of 'positive obligations', which turns the obligation of the governmental authorities from one of merely refraining from violating privacy rights into an active duty to protect those rights of individuals. This, therefore, extends the protection to individuals against private third parties.[19]

This is, however, only the status at the European level. In the case of Mount Athos, clearly the Greek authorities protected the privacy of the monasteries and surrounding areas over an individual's right of free information gathering. However, that is indeed a matter to be decided upon at the national level – other states might have decided differently in comparable circumstances, either in terms of national laws or statutes, or in terms of court decisions in case of actual disputes.

A further point of note concerns the scope of "everyone", as the subject entitled to the rights of Article 8(1): does it include juridical persons?[20] Drafted so as to address natural persons only, originally considerable uncertainty existed as to whether it could nevertheless be interpreted to apply to juridical persons as well. However, with the 2002 *Colas Est* case, that question has been settled with an affirmative answer.[21] As such, companies, whose right to 'privacy' would be violated by VHR satellite data, might – if falling otherwise within the scope of the European Convention of course – base a relevant claim upon Article 8.

Finally, questions could still arise as to the scope of the notions of 'privacy' and 'interference' therewith, specifically also as to the role satellite data could play in this context.

Prosser's Law of Torts, for example, lists four categories of relevant

---

[18] See further also *Velu*, *supra* note 15 at 20-3, 87-91.

[19] See *Van Dijk*, *supra* note 16 at 739-45.

[20] See *Velu*, *supra* note 15 at 18-20.

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

interference: (1) intrusion on plaintiff's privacy; (2) public disclosure of private facts; (3) putting the plaintiff in a false light in the public eye; and, (4) appropriation of some elements of the plaintiff's personality for the defendant's advantage.[22]

It seems that (1) and (2) would be at issue in the case of VHR satellite data: those data could well intrude upon any privacy as long as they concern open air activities, and could similarly be disclosed to the public fairly easily. Many VHR satellite data applications are of a commercial character, making their providers interested in spreading them in principle as widely and as easily as possible. In addition, it could be imagined that cases might fall within category (3), in particular when satellite data might be tampered with.

In May 1967, considering the right to privacy, the Nordic Conference of Jurists arrived at a wider definition as follows:[23]

> The right of the individual to lead his own life protected against: (a) Interference with his private, family and home life. (b) Interference with his physical or mental integrity or his moral or intellectual freedom. (c) Attacks on his honour and reputation. (d) Being placed in a false light. (e) The disclosure of irrelevant, embarrassing facts relating to his private life. (f) The use of his name, identity or likeness. (g) Spying, prying, watching and besetting. (h) Interference with his correspondence. (i) Misuse of his private communications, written or oral. (j) Disclosure of information given or received by him in circumstances of professional confidence.

From the perspective of VHR satellite data, more or less similar to the case of Prosser's abovementioned definition, categories (a) and (e) clearly apply, at least in principle. In addition, category (g), absent as a specific category in Prosser's definition, should be noted: this category includes persistent watching of a person, photographing and filming, eavesdropping and recording. Subject to limited exceptions relating to consent of the targeted individual or any public nature or function in which the target was active,[24] this category would include cases where

[22] As discussed in *Velu*, *supra* note 15 at 32-3.

[23] As quoted in *Velu*, *supra* note 15 at 33.

[24] See *Velu*, *supra* note 15 at 51-58. Exceptions regarding the target's consent, it may be noted, may lead to additional problems of interpretation in the context of satellite data, as in most cases the target will not be aware that a satellite is generating data of potential particular concern to him.

fundamental use is made of observation satellites.

As indicated above, no exhaustive authoritative list of activities, scenarios or situations has been developed for the definition of 'private life', the phrase within Article 8 most relevant in the context of VHR satellite data. The closest to such a list came in the judgment of the European Court of Human Rights in the *Pretty* case:[25]

> As the Court has had previous occasion to remark, the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person . . . . It can sometimes embrace aspects of an individual's physical and social identity . . . . Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 . . . . Article 8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world . . . . Although no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees.

One authoritative expert text interprets this to mean that Article 8 contains "various guarantees to personal autonomy, personal privacy, personal identity, personal integrity, personal development, personal identification and similar concepts linked to the individual notion of personhood".[26]

In any event, "the registration of personal data has been a vital issue of the notion of privacy" – a conclusion of clear relevance for VHR satellite data.[27] The obligations under Article 8, however, seem to be indeed directed largely to governmental authorities (such as in the medical field), although sometimes private institutions of a specific non-commercial nature could also become involved.[28]

A second notion of potential relevance for activities involving VHR satellite data concerns the respect for the home and protection

---

[25] *Pretty*, *supra* note 16 at § 61.

[26] *Van Dijk*, *supra* note 16 at 665.

[27] *Van Dijk*, *supra* note 16 at 666; see also 667-79 for further analysis.

[28] See also *Van Dijk*, *supra* note 16 at 667-77.

against nuisance, which "also include those [violations of the right] that are not concrete or physical, such as . . . other forms of interference".[29] The right, in particular in VHR-data related circumstances, may actually be difficult to distinguish from the right to private life.[30] Still, it has apparently not been made clear so far whether virtual interference with the right, 'spying' as such (that is without further concrete nuisance resulting from such spying, for example a publication on the web of the VHR data concerned) would already constitute a violation of Article 8 of the Convention.

Finally, it should be noted that the rights offered by Article 8 of the European Convention are not unlimited.[31] Specific limitations are already offered by the Convention itself, referring to "time of war or other public emergency threatening the life of the nation",[32] "the political activity of aliens",[33] as well as national security, public safety and other exceptions explicitly provided for by Article 8.

III. THE EUROPEAN COMMUNITY AND PRIVACY: THE ECONOMIC APPROACH

In quite clear contrast to the Council of Europe and the European Convention on Human Rights, the European Community ultimately became involved in privacy protection issues from an economic perspective. This is ultimately not surprising since the Community had originated from the need for general economic integration of the member states by means of regulation, even if the scope of involvement of the European authorities and EC law has, over the decades, extended so as to encompass many areas not of a (purely) economic nature.

It became apparent that the application of privacy protection could often impact negatively upon economic activities.

Without trying to sum up the comprehensive legislative development of the EC legal order here, it may be helpful to reiterate the official aims of the European Community, then Union, as they were defined by Article 2 of the EC Treaty,[34] in order to assess the potential for

---

[29] *Van Dijk*, *supra* note 16 at 719.

[30] See also *Van Dijk*, *supra* note 16 at 723.

[31] See especially *Velu*, *supra* note 15 at 66-87.

[32] *European Convention on Human Rights*, Art. 15(1).

[33] *European Convention on Human Rights*, Art, 16.

[34] The EC Treaty is essentially the original Treaty of Rome, or *Treaty establishing the European Economic Community*, Rome, done 25 March 1957, entered into force 1 January 1958; 298 UNTS

privacy issues to come within the scope of that Treaty's regime. Such aims and objectives include: the development of the EC economy; a high level of employment and social protection; a high level of environmental protection; the enhancement of the standard of living throughout the member states; and the economic and social cohesion of the Community and its member states.[35]

The consequence of an absence of a reference to 'privacy' in the EC Treaty (or any other part of primary EC law) is that EC law only interferes once privacy protection or, in a wider sense, privacy issues, would have a certain negative impact on economic activities. If such a negative impact is determined to exist, the EC authorities – the Commission, the Parliament and the Council in a complicated interplay of roles, responsibilities and competencies in the creation of EC law – can come up with the necessary Regulations, Directives and/or Decisions to curb such negative impacts. Such an Internal Market-perspective has caused EC legislative activities over the decades to be particularly focused on three areas.[36]

The first area concerns the realization of the so-called four freedoms of cross-border movement: of goods (products),[37] persons (as far as they are involved in economic activities and, for that purpose,

---

11; as it was fundamentally amended by the Treaty on European Union, Maastricht, done 7 February 1992, entered into force 1 November 1993; 31 ILM 247 (1992); OJ C 191/1 (1992). The *Treaty of Amsterdam Amending the Treaty on European Union, the Treaties Establishing the European Communities and Certain Related Acts* (hereafter Treaty of Amsterdam), Amsterdam, done 2 October 1997, entered into force 1 May 1999; OJ C 340/73 (1997); then *inter alia* resulted in a major renumbering exercise; the numbering of Articles in the present contribution is the one following that renumbering. [EC Treaty].

[35] Art. 2 EC, (that is in its version as per the Treaty of Amsterdam) reads in full: "The Community shall have as its task, by establishing a common market and an economic and monetary union and by implementing common policies or activities referred to in Articles 3 and 4, to promote throughout the Community a harmonious, balanced and sustainable development of economic activities, a high level of employment and of social protection, equality between men and women, sustainable and non-inflationary growth, a high degree of competitiveness and convergence of economic performance, a high level of protection and improvement of the quality of the environment, the raising of the standard of living and quality of life, and economic and social cohesion and solidarity among Member States."

[36] From an overarching perspective, a fourth area has traditionally been that of 'external competence', i.e. the possibility at the European level to override individual member state actions *vis-à-vis* third states, in terms of regulating or deregulating trade and other economic relations with such third states. From the perspective of the current contribution, however, this area does not need much attention at this point in time.

[37] *EC Treaty*, Art. 23.

interested in moving across intra-EU borders),[38] services[39] and capital.[40] From a privacy perspective, the protection thereof could be seen to potentially interfere with all four freedoms. From a remote sensing perspective, it would largely depend on whether one considers remote sensing and the provision of remote sensing information to be a service or to be about delivery of a product (a dataset, for example).

In practice, where remote sensing is considered to amount to a service, EC law may require EU member states to allow the providers of such services, irrespective of their nationality, to offer them in their respective territories on the same condition as home-grown providers would do. *Mutatis mutandis*, if remote sensing is essentially about the production of 'goods' such as datasets, then EC law might operate so as to ensure the free movement of such goods across intra-EU borders. In either case, it is not the activity in outer space or the production of datasets as such which would be the subject of the Community's legal attention, only downstream aspects within the Community itself. In either case, also, it is in this context that EC law might also come to interfere with the protection of privacy.

A second, much more focused area of EC law concerns what is commonly referred to as the 'competition' or 'anti-trust' regime, the essence of which is to try and ensure a level playing field for private companies throughout the European Union by means of dedicated instruments curbing anti-competitive behavior. These instruments are basically of a twofold nature.

One set is addressed directly at private undertakings, for example prohibiting market strategy coordination ('cartels' or 'collusive conduct' as it is now labeled), to the extent that such coordination would have a substantive negative effect on this EU-wide level playing field.[41] Moreover, this set of rules seeks to outlaw the abuse of a dominant position (such as a monopoly) that a particular private company may have for anti-competitive purposes.[42]

The other set is addressed to member states, to the extent that they might wish to provide state aid to (private) undertakings in order to favor certain undertakings over others, and hence distort the proper

[38] *EC Treaty*, Art. 39.
[39] *EC Treaty*, Art. 49.
[40] *EC Treaty*, Art. 56.
[41] *EC Treaty* Art. 81.
[42] *EC Treaty* Art. 82.

functioning of the Internal Market.[43]

From the perspective of privacy, it could perhaps be expected that as soon as laws or regulations enunciated by national authorities dealing with the protection of personal data would result in a distortion of free competition and the level playing field, such instruments of competition law could be called upon to remedy that distortion. However, upon closer view, this only plays at the level of national legislation of member states. Thus, in reality, the envisaged Internal Market consists of various national markets fenced off by major differences in levels of protection.

This brings us to the third area of EC law which seeks to address privacy concerns: harmonization of national laws to make sure that both private companies and private persons are provided or entitled to roughly the same level of protection throughout the Union. In fact, a considerable degree of legislation has been created under this heading to address the matter.

From the EU perspective, the internal and fundamental objectives of the European Union will necessarily lead to a substantial increase in cross-border flows of personal data. The main issue underlying legislative actions at the EC level with respect to the protection of data for privacy protection purposes is that such data may, on the one hand, become available to the public (which is in line with the general goals and purposes of EU policies regarding free trade and open and fair competition) but, on the other hand, they may interfere with the right to privacy - which is also a general principle of law acknowledged and respected in EC law. Thus, the legal discussion focuses on the balance between free provision and movement of information on the one hand and the protection privacy rights on the other.

As long as space-borne data are to be considered as data impinging on a person's privacy, the main question for satellite remote sensing is to what extent further generation, processing, handling and distribution of those data that may result in public accessibility would be lawful.

---

[43] *EC Treaty* Art. 87.

IV. THE BASELINE REGIME FOR THE EUROPEAN UNION: THE DATA PROTECTION DIRECTIVE

A. THE DATA PROTECTION DIRECTIVE: SCOPE, OBJECTIVES AND DEFINITIONS

The first major result of the drive within the Community to harmonize the national regimes regarding privacy and data protection where the absence of such harmonization might interfere with the proper functioning of the Internal Market was Directive 95/46/EC of October 1995, also known as the Data Protection Directive.[44] The approach of this central piece of Community-legislation makes it clear that the issues concerned are addressed very much from the traditional EC-angle: "the Directive shall not apply to the processing of personal data . . . in the course of an activity which falls outside the scope of Community law".[45]

The objectives of Directive 95/46 are, firstly, that EU member states shall protect the fundamental rights and freedoms of natural persons, and in particular, their right to privacy with respect to the processing of personal data.[46] Secondly, member states shall neither restrict nor prohibit the free flow of personal data between member states merely out of an interest to afford protection as envisaged under the Directive's regime.[47] In other words: privacy arguments may not be (ab)used to distort the functioning of the EU Internal Market.

Currently, EU member states do not offer the same "level of protection of the rights and freedoms of individuals, notably the right to privacy".[48] This aspect may prevent "the transmission of personal data from the territory of a Member State to that of another Member State"; a difference which may "therefore constitute an obstacle to the pursuit of a number of economic activities at Community level, distort competition and impede authorities in the discharge of their responsibilities under Community law".[49]

---

[44] EC, *Directive of the European Parliament and of the Council* 95/46/EC *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. [Directive 95/46].
[45] *Ibid.*, at Art. 3(2).
[46] *Ibid.*, at Art. 1(1).
[47] *Ibid.*, at Art. 1(2).
[48] *Ibid.*, at Recital 7.
[49] *Ibid.*, at Recital 7.

The overarching aim of Directive 95/46 is thus to promote equivalent levels of protection of the rights and freedoms of individuals among member states. This allows safe cross-border flow of personal data in parallel with equivalent and safe levels of protection of privacy rights. Approximation of national laws is ensured in the Directive, but member states are left some margin for maneuver, being able to specify in their national law the general conditions governing the lawfulness of data processing.

The principle of protection must be reflected in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out.

With a view to investigating to what extent satellite-derived data might fall within the scope of the EC regime outlined above, reference should be had next to the rather all-encompassing definitions of eight key concepts and terms. These concepts concern the application of the Directive, as well as that of further EC legal documents, as they indicate the general approach and scope of the regime concerned.

These key concepts are defined as follows:[50]

> (a) 'personal data' shall mean any 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;
> (b) 'processing of personal data' hereinafter referred to as 'processing' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
> (c) 'personal data filing system' hereinafter referred to as 'filing

[50] *Ibid.*, at Art. 2. It may be noted that the exact same definitions reappear in one of the follow-up EC-law documents; see EC *Regulation of the European Parliament and of the Council* 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* [2001] O.J. L 8/1 at Art. 2. [Regulation 45/2001].

system' shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
(d) 'controller' shall mean the Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Community act, the controller or the specific criteria for its nomination may be designated by such Community act;
(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;
(f) 'third party' shall mean a natural or legal person, public authority, agency or body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;
(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed.

From a practical point of view, a provider of satellite-derived products and/or services would be most analogous to the 'controller' or the 'processor' under the Directive's terms. Such a controller or processor can be any "natural or legal person, public authority, agency or any other body".[51] The, generally speaking, broad definitions of 'personal data' and 'processing of personal data' leave ample room for VHR satellite data to be included, and hence subjected to the regime of the Data Protection Directive.

B. THE REQUIREMENTS IMPOSED BY THE DATA PROTECTION DIRECTIVE ON DATA HANDLING

The Directive thus envisages data in a very wide sense. Given the

[51] *Directive 95/46*, Art. 2(d).

developments under way, in the framework of the information society, of increasingly refined techniques used to capture, transmit, manipulate, record, store or communicate sounds and image data relating to natural persons, the Directive should be applicable in principle to any processing activities involving any such satellite data. The Directive shall therefore also apply to any processing of remote sensing data, whether automatic or in order to form part of a filing system, as long as a service provider can access the positioning and navigation data. However, such processing is then subjected to a number of requirements in order to be lawful under the Directive:[52] personal data must be:

- processed fairly and lawfully;
- collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that member states provide appropriate safeguards;
- adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member states shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use."

In addition:[53]

Personal data may be processed only if:

- the data subject has unambiguously given his consent; or
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a

[52] *Ibid.*, at Art. 6(2).
[53] *Ibid.*, at Art. 7.

contract; or
- processing is necessary for compliance with a legal obligation to which the controller is subject; or
- processing is necessary in order to protect the vital interests of the data subject; or
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).

Additionally, a distinction is provided between cases of collection of data from the data subject, dealt with by Article 10, and cases where the data have not been obtained from the data subject, which is usually the relevant scenario for satellite data, especially if the satellite data is not enhanced, validated and/or verified by terrestrial data and information collection. In such cases:[54]

> the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:
>
> 1. the identity of the controller and of his representative, if any;
> 2. the purposes of the processing;
> 3. any further information such as
>   - the categories of data concerned,
>   - the recipients or categories of recipients,
>   - the existence of the right of access to and the right to rectify the data concerning him
>
> in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

Further clauses then deal with the actual security of processing

[54] *Ibid.*, at Art. 11(1).

personal data with potentially privacy-sensitive impacts, such as the implementation of appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of processing. Moreover, it establishes an obligation for the data controller to provide sufficient guarantees in respect of such technical security measures and organizational measures governing the processing to be carried out, and to ensure compliance with those measures.[55]

Furthermore, when a processor is involved, the activities should be regulated by a contract or legal act binding the processor to the controller, stipulating in particular that:

> the processor shall act only on instructions from the controller, and relevant obligations, as defined by the law of the EU member state in which the processor is established, shall also be incumbent on the processor'.[56]

The Directive applies to "the processing of personal data wholly or partly by automatic means and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system".[57] This is done "so as to permit easy access to the personal data in question".[58]

However, there are a few exceptions limiting such comprehensive application. Directive 95/46 provides for some prohibited categories of data processing, listed as covering "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life".[59] Satellite data somehow giving away someone's position are not included in this list merely for that reason, generally speaking, VHR satellite data will not fall within the above prohibited categories.

One further relevant exception here concerns data processing for statistical, historical or scientific purposes.[60] Such data are offered no protection under the Directive in terms of limiting or prohibiting access

---

[55] *Ibid.*, at Art. 17(1) & (2).
[56] *Ibid.*, at Art. 17(3).
[57] *Ibid.*, at Art. 3(1).
[58] *Ibid.*, at Recital 15.
[59] *Ibid.*, at Art. 8(1).
[60] *Ibid.*, at Art. 11(2).

to them, subject to some guarantees ensuring a proper and balanced application of this clause.

Furthermore, according to its own terms, "the Directive shall not apply to the processing of personal data . . . in the course of an activity which falls outside the scope of Community law, such as those provided for by Title V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation related to State security matters) and the activities of the State in areas of criminal law", by a natural person in the course of a purely personal or household activity.[61] Such data does not enjoy the protection offered by the Directive either.

These exceptions for public security, defence, state security and criminal law-related activities are noteworthy as they provide a major *caveat* to the application of the Directive's regime to the remote sensing environment. Thus, for example, the processing of satellite data, even if 'personal' in the sense of the Data Protection Directive, does not fall within the scope of the Directive where such processing relates to state security matters.

This exception may have a particular impact on VHR satellite data processing as many such data will result from activities conducted for purposes of public safety, defence or state security. This, obviously, would have to be clearly indicated, and this clause ought to be interpreted in a manner which avoids abuse of its potential application.

To be precise however, the consequence of this provision is not that *no* restrictions protecting privacy interests apply in this context, but rather that all and any such restrictions are still basically imposed by national legislation and for domestic purposes (and at a more general level by international and European human rights law).

Thus, Directive 95/46 provides the baseline regime for dealing with privacy issues within the European Union and its EC law framework. The Directive itself directly refers to the relevant internal and fundamental objectives of the European Union:[62]

creating an ever closer union among the peoples of Europe,

---

[61] *Ibid.*, at Art. 3(2).
[62] *Ibid.*, at Recital 1.

> fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognised in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.

That baseline was soon seen to require specific elaboration in three particular areas: (1) where EU institutions themselves would come to play a key role in the process of data generation, gathering, processing and/or dissemination; (2) to the extent telecommunications infrastructure would present the logical means for distribution and dissemination also of satellite data with potential privacy-sensitive effects; and (3) the extent to which the substance of the EC law regime could and/or should be effectively transported outside the Union in order to protect the interests of the whole legal framework within the Union.

V. THE ELABORATIONS: EU INSTITUTIONS, TELECOMMUNICATIONS AND EXTRA-EU EFFECTS

A. REGULATION 45/2001 – EU INSTITUTIONS INVOLVED IN DATA HANDLING

Regulation 45/2001[63] essentially applies, and where necessary adapts, the regime of Directive 95/46 to the main organs and bodies of the European Community and European Union itself. Thus, its scope is to "provide the individual with legally enforceable rights to specify the data processing obligations of the controllers within the Community institutions and bodies and to create an independent supervisory authority responsible for monitoring the processing of personal data by the Community institutions and bodies".[64]

The role and responsibilities of the controller as determined by Directive 95/46 shall therefore, as a consequence of Regulation 45/2001, also apply to EU institutions and bodies. The "controller shall mean the

---

[63] *Regulation 45/2001*, *supra* note 51.
[64] *Ibid.*, at Recital 5.

Community institution or body, the Directorate-General, the unit or any other organizational entity which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by a specific Community act, the controller or the specific criteria for its nomination may be designated by such Community act".[65]

The most important difference to Directive 95/46 is embodied in the clauses on the lawfulness of processing, making data processing legitimate only as far as:[66]

> necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed, or . . . necessary for compliance with a legal obligation to which the controller is subject, or to take steps at the request of the data subject prior to entering into a contract, or [when] the data subject has unambiguously given his or her consent, or . . . necessary in order to protect the vital interests of the data subject.

Transfer of personal data – whether within or between EU institutions or bodies, or to recipients, other than EU institutions or bodies, subject to Directive 95/46, or to recipients, other than EU institutions or bodies, which are not subject to Directive 95/46 – in principle shall be legitimate as long as carried out in the public interest.

While *prima facie* it is unlikely that EU institutions would be crucially involved in data handling operations themselves, the recent arrival on the space scene of the Global Monitoring for Environment and Security initiative (GMES) (recently re-christened Kopernikus) may change that very soon.

In November 2001, an EU Council Resolution called for the European Commission to coordinate with ESA to develop "an operational and autonomous European capability for global monitoring for environment and security" by 2008, crucially involving a satellite

---

[65] *Ibid.*, at Art. 2(d).
[66] *Ibid.*, at Art. 5,

system.[67] This capability was to result in an infrastructure of interoperability, with standardized databases being filled with relevant data. These data would be partly self-generated by the key GMES players, notably ESA and EUMETSAT, with EUMETSAT being considered another major stakeholder even though not, to date, an 'official' partner in the project.

However, the details of the institutional and governance structure to be established at the core of the GMES/Kopernikus initiative remain subject to discussion. At some point the establishment of a core entity, provisionally labeled 'GMES Authority', must be envisaged. The extent to which existing legal rules on privacy protection under Regulation 45/2001 would apply in the GMES/Kopernikus context depends to a considerable extent on the legal character and personality of such a GMES Authority (or similar body or bodies). A number of options have already entered the debate on this issue, generally referring to various types of bodies or organs that can be established under EC law such as a Joint Undertaking,[68] an Executive Agency,[69] a Community Agency[70] or a Joint Technology Initiative (JTI).[71]

---

[67] EC, Council Resolution on the launch of the initial period of global monitoring for environment and security (GMES) [2001] O.J. C 350/4 at para (3). See further EC, Communication from the Commission to the European Parliament and the Council – Global Monitoring for Environment and Security (GMES): Establishing a GMES capacity by 2008, [2004] COM(2004) 65;. See e.g. Frans G. von der Dunk, 'The 'S' of 'Security': Europe on the Road to GMES' (2007) 4-2 *Soochow Law Journal* at 1.

[68] EC Treaty Art. 171. See e.g. Communication of 3 February 2004, 17. The example usually referred to, of course, is the Galileo Joint Undertaking that paved the way for the Galileo development, deployment and operational phases.

[69] EC, Council Regulation 58/2003/EC laying down the status for executive agencies to be entrusted with certain tasks in the management of Community programmes [2002] O.J. L 11/1; See also EC, Commission Decision 2004/20/EC setting up an executive agency, the 'Intelligent Energy Executive Agency', to manage Community action in the field of energy in application of Council Regulation (EC) No 58/2003 [2004] O.J. L 5/85; EC, Commission Decision 2004/858/EC setting up an executive agency, the 'Executive Agency for the Public Health Programme', for the management of Community action in the field of public health – pursuant to Council Regulation (EC) No 58/2003, [2004] O.J. L 369/73.

[70] See e.g. European Environment Agency (EEA), established by EC, Council Regulation 1210/90/EEC on the establishment of the European Environment Agency and the European Environment Information and Observation Network, [1990] O.J. L 120/1; European Aviation Safety Agency (EASA), established by Regulation of the European Parliament and of the Council 1592/2002/EC on common rules in the field of civil aviation and establishing a European Aviation Safety Agency, [2002] O.J. L 240/1; European Maritime Safety Agency (EMSA), established by Regulation of the European Parliament and of the Council 1406/2002/EC establishing a European Maritime Safety Agency, [2002] O.J. L 208/1.

[71] See Communication from the Commission to the Council and the European Parliament – European Space Policy – Preliminary Elements, SEC(2005)664, Brussels, 23 May 2005,

Whilst other options – such as creating an altogether new intergovernmental organization for the purpose – have also been considered, the aforementioned options would utilize an EU institution and, therefore, the regime developed under Regulation 45/2001 would impact upon Kopernikus' activities to that extent.

Without having formally clarified the issue, more recent legal documents on GMES/Kopernikus have only fuelled the expectation that the future key players in the initiative and the institutional framework to be established for it would include one or more EU institutions. For instance, the Communication of 10 November 2005, aptly entitled 'From Concept to Reality',[72] starts by reiterating the general thrust of the GMES project. Thus, it states: "the need for reliable and timely information has been underlined by increased demand. Natural and manmade catastrophes in Europe, America, Asia and Africa, coupled with increased security needs, have further reinforced the case for improved monitoring systems. Global to local levels of requirements have now been identified".[73]

GMES/Kopernikus is thus tasked to support a range of EU policies, and the Communication refers specifically to concrete examples like the Union's involvement in agriculture, environmental and fisheries monitoring, external relations such as in case of disaster and emergency response action, and development policies.[74] The Communication further determines the way forward by means of defining the concepts of 'pilot operational services' and 'Fast Track introduction'.[75]

COM(2005) 208 final.

[72] 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. [Concept to Reality]. Whilst the GMES website makes reference to a further Decision of the Commission of 8 March 2006, pertaining to the establishment of a core team on GMES labelled the 'GMES Bureau', at the time of this writing it has not been possible to locate and access that Decision; see online: <http://www.gmes.info/72.0.html>. accessed 28 July 2008, last updated 17 November 2006.

[73] *Concept to Reality*, *ibid*., at 5.

[74] *Ibid*., at, 6-7.

[75] The focus on institutional users, notably EU institutions and national governments, as potential output receivers, is further reflected in the membership of the various groups established to develop the three fast track services. The Emergency Response Core Service (ERCS) Implementation Group thus comprises the Italian Civil Protection agency representing national EU member states' civil protection agencies, the Commission's DG's on Environment and External Relations respectively, the Commission's Humanitarian Aid Office (ECHO) and the fire rescue service of the Czech Republic representing the civil

The key role of GMES/Kopernikus in supporting EU policies, the involvement of many Commission Directorates-General in the pilot operational services and the general political leading role of the Commission in the effort makes it likely that an EU institution will function as a key entity within the operational framework for GMES. Moreover, the same and/or other EU institutions will also be playing important roles in downstream dissemination, which is where – in the case of VHR satellite data at least – privacy issues may start to arise. As such, an EU institution or body would qualify as a 'GMES data controller'.

Thus, the legal regime developed on the basis of the Data Protection Directive and further elaborated for this special case by Regulation 45/2001 would mean, in the context of GMES, that transfer of personal data for *commercial* purposes may not be possible.

B. DIRECTIVES 97/66 AND 2002/58 – TELECOMMUNICATIONS INVOLVED IN DATA HANDLING

In view of the key role telecommunication services and infrastructure play in today's issues of privacy and privacy-sensitive access to data, a special set of EC law instruments have been developed for the purpose. In this context, the first such instrument that dealt with the issue, Directive 97/66,[76] focused on the processing of personal data and the protection of privacy in the telecommunications sector in a rather comprehensive fashion. Given the prominent use of telecommunications infrastructure for the dissemination and distribution of satellite remote sensing data, this instrument of EC law is particularly relevant for the current analysis.

---

protection agencies in new EU member states; see online: <http://www.gmes.info/168.0.html>. accessed 28 July 2008. The Land Monitoring Core Service (LMCS) Implementation Group likewise comprises the German national mapping agency, the Hungarian Institute of Geodesy, representing user communities in new EU member states, the European Topic Centre on Terrestrial Environment, the European Environmental Agency, and the Commission's DG's on Regional Policy respectively Agriculture and Rural Development; see online: <http://www.gmes.info/167.0.html>. accessed 28 July 2008. The Marine Core Service (MCS) Implementation Group finally comprises the European Association for the Global Ocean Observing System 'EuroGOOS', European Meteorological Offices, the Marine Board of the European Science Foundation, the Commission's Maritime Policy Task Force, the European Environment Agency, the European Maritime Safety Agency and the Commission's DG on External Relations; see online: <http://www.gmes.info/169.0.html>. accessed 28 July 2008.

[76] EC, *Directive of the European Parliament and of the Council* 97/66/EC *concerning the processing of personal data and the protection of privacy in the telecommunications sector*, [1998] O.J. L 24/1.

The aim and objective of Directive 97/66 was to create rules that were technology-neutral, that is, they were not to dictate or discriminate in favor of the use of a particular type of technology. Rather, they ought to ensure that the same service is regulated in an equivalent manner irrespective of the means by which it is delivered. Directive 2002/58[77] was then drafted to replace Directive 97/66 concerning the processing of personal data and the protection of privacy in the telecommunications sector in order to adapt and update the existing provisions to new and foreseeable developments in electronic communications services and technologies, notably of ICT (information and computer technology) convergence.

Thus, Directive 2002/58 provides for the harmonization of the provisions of the member states, who are required to ensure an equivalent level of protection of fundamental rights and freedoms within the EU, and in particular the right to privacy, with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of such data and electronic communications equipment and services within the European Union.[78] The Directive applies to the processing of personal data specifically in connection with the provision of publicly available electronic communications services in public communications networks. It seeks to provide suitable measures for adaptation of previous EC legal measures to developments in the markets and technologies for electronic communications services. It does this in order to provide an equal level of protection of personal data and privacy for users of publicly available electronic communications services, regardless of the technologies used.

The existing definitions of 'telecommunications services and networks' under Directive 97/66 were subsequently replaced in Directive 2002/58 by the definition 'electronic communications services and networks' under Article 2. This is to ensure that all different types of transmission services for electronic communications will be covered regardless of the technology used, and essentially in the same, technology-neutral fashion.

Moreover, four new definitions were added, of "calls", "communication", "traffic data", and "location data" respectively, to

[77] EC, *Directive of the European Parliament and of the Council* 2002/58/EC *concerning the processing of personal data and the protection of privacy in the electronic communications sector*, [2002] O.J. L 201/37. [Directive 2002/58].,
[78] *Ibid.*, at Art. 1(1) & (2).

strengthen the common understanding of these terms and thereby improve the harmonized implementation of the relevant articles throughout the European Union.[79]

The provisions of these Directives thereby particularize and complement Directive 95/46 for the purposes of the "processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community".[80] Also, these provisions provide for the protection of legitimate interests of legal persons: Directive 2002/58 considers legal persons to be persons whose interests can and should indeed be legitimately protected.

Confidentiality of communications including the relevant traffic data and the prohibition of tapping or other forms of surveillance by third parties are also guaranteed:[81]

> (1) Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.
> (2) Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

As it is very important for data subjects to be fully informed about the type of data which are being processed and the purposes for which this is done, an explicit obligation is imposed by the Directive to inform

---

[79] *Ibid.*, at Art. 2(e), (d), (b) & (c).
[80] *Ibid.*, at Art. 3(1).
[81] *Ibid.*, at Art. 5,

subscribers of the data which are being collected.[82] This empowers subscribers to any service involving substantial data generation and handling to control and, where necessary, object to ongoing data processing.

The impending arrival of Europe's second-generation satellite timing, positioning and navigation system Galileo on the European scene has caused necessary amendments to the existing regime.[83] Not only is this of interest to GMES/Kopernikus given the potential for satellite positioning information to enhance the precision and value of GMES data, it has also caused the EC to enact a new article on location data other than traffic within Directive 2002/58. It stipulates that such data:[84]

> may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time.

The only exceptions to the principle of prior consent would be the use of location data by emergency services as well as the existing derogation for EU member states for the purposes of public and national security and criminal investigations. For these purposes a reference is included in Article 15(1) of Directive 2002/58 to allow member states to restrict the of use location data where this is necessary and proportionate.

Lastly, the Directive provides for clauses on technical features and standardization, guaranteeing that data protection considerations may not lead to trade and service barriers within the EU Internal Market for

---

[82] *Ibid.*, at Art. 6(4).

[83] See e.g. Frans G. von der Dunk, "Towards Monitoring Galileo: the European GNSS Supervisory Authority" in *statu nascendi*, (2006) 55 Zeitschrift für Luft- und Weltraumrecht 100; See also Frans. G von der Dunk "Hosting Galileo Ground Stations – Liability and Responsibility Issues under Space Law" in *Proceedings of the Fiftieth Colloquium on the Law of Outer Space* (2008) 358.

[84] *Directive 2002/58*, *supra* note 78 at Art. 9(1).

terminal equipment and software and ensures that any mandatory requirements on terminal equipment and software to protect personal data and privacy may only be imposed through EC procedures.[85]

Exceptions to the application of the general regime of Directive 95/46 remain possible, however. EU member states may restrict provisions of the Directive to safeguard public security and conduct criminal investigations. Moreover, such exceptions extend to situations "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e., State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC".[86] Again, the relevance for satellite remote sensing activities, in particular GMES / Kopernikus, will be clear.

Finally, Article 1(3) of Directive 2002/58 provides for the same exceptions as Directive 95/46 regarding Title V and VI of the Treaty of the European Union, regarding public and national security and criminal investigations. The Directive provides for very specific obligations here, *inter alia* imposing responsibility for the security of services and networks on providers and obliges them to inform subscribers in case of residual security risks:[87]

> (1) The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
> (2) In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

---

[85] *Ibid.*, at Art. 14.
[86] *Ibid.*, at Art. 15(1).
[87] *Ibid.*, at Art. 4.

In sum, such general obligations pertaining to the use of telecommunication infrastructure under Directive 2002/58 with a view to privacy issues will also have a fundamental impact on VHR satellite data downstream services and activities, in view of the almost inherent need for the latter to make use of such infrastructure.

C. DECISIONS 2001/497 AND 2002/16 – EXTRA-EU EFFECTS OF DATA HANDLING

The extent to which personal data is protected outside the European Union, whether for privacy purposes or for other purposes, is fundamentally a matter for national legislation of the states where such protection is desired; obviously, the EU institutions cannot determine any applicable principles and rules outside the territories of the EU member states.

Nevertheless, the European Union has the competencies to deal with such issues to the extent that EU entities and companies, including notably a GMES Authority for Kopernikus, are involved in such dealings. Two Decisions of the European Commission are relevant in this respect: Decision 2001/497 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46,[88] and Decision 2002/16 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46.[89]

Since most satellite remote sensing activities have a tendency of being of global effect, scope and application, EC law such as the aforementioned Decisions relating to data protection will apply even for data transfers outside Europe, as long as the data processing itself is performed under the jurisdictions of one or more EU member states.

For any satellite-data-based activities downstream of any European satellite operator and/or GMES Authority in these states the regime of Directive 95/46 continues to apply, *mutatis mutandis*. To the extent that such operators have the legal nationality of (that is place of incorporation and headquarters in) an EU member state, or operate from

[88] EC, Commission Decision 497/2001/EC on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, [2001] O.J. L 181/19.

[89] EC, Commission Decision 16/2002/EC on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, [2002] O.J. L 6/52.

EU member state territory, they would be equally bound by such rules. The same applies to any satellite remote sensing data and/or service provider operating in the EU markets. This is the case even if the provider is non-EU in origin and conducting their operations basically from outside the European Union, regardless of whether they use data derived from European satellites or not. The aim must ultimately be to maintain a level playing field within the European Union.

If, however, non-EU companies not operating from EU territory would become customers for European satellite-derived data or customers for services so as to incorporate these the services the non-EU companies perform outside EU territory, relevant entities would have a 'flow-down' duty to ensure that it will in no way contribute thereby to circumvention of this EU regime.

To this extent, the effects of the EC law regime discussed could be labeled as 'extra-territorial'. Obviously, if in such a case a non-EU customer would obtain data without any involvement of European satellite products or services, and handle them differently from that which would be allowed under the EU regime, there is – legally speaking – little either the GMES Authority or the Commission or even the EU member states could do about it. However, the burden of proof that the relevant authority was not able to prevent that from happening would lie with the authority – the GMES Authority in case of Kopernikus, the Commission and/or individual EU member states, as applicable. Of course, any such event may lead to undesirable political fall-out.

The extent to which this general legal framework will in practice affect European VHR satellite data operations and downstream activities can of course only be determined in fairly general terms, noting that even in the context of GMES / Kopernikus major uncertainties regarding the structural framework for operations and downstream activities still exist.

VI. CONCLUDING REMARKS

Comparing the two 'European approaches', it is clear that they come from rather different points of departure; and stay true to those. On the one hand, there is the legal framework developed under the auspices of the Council of Europe which views privacy as a rather fundamental human right, to be protected against all undue interference, including commercial ones. On the other hand, the law developed within

the European Community starts out from a commercial vantage point and tries to ensure that a level playing field with open borders exists also in areas where privacy concerns may come to obstruct or limit access to data, including VHR satellite data.

Aggravating the potential conflict between those two approaches, the two international organizations have a different set of states as members; the Council of Europe counting 47 member states altogether, the European Union counting 27.

Nonetheless, such potential conflicts are mitigated firstly by the fact that all EU member states are members of the Council of Europe. Secondly, even where divergence between the Council of Europe-member states not members of the Union and those that are members of the Union may arise, it should be pointed out that the Community itself and its institutions are committed to upholding the obligations imposed by the European Convention on Human Rights. As such, EC law is to respect and, where required, even incorporate the core substance of the Convention's system of human rights protection into its day to day influence within 'Europe'.[90]

Therefore, within the context of EC law, the protection of the individual constitutes the principle whereas the free flow of information, deemed necessary for optimal economic and commercial development, constitutes the exception. This is clearly contrary to its official relationship being the other way round. The undue obstruction of the Internal Market and furtherance of commercial activities on a level playing field remain the primary focus of EC law, leading to harmonization efforts such as those discussed above. Yet, ultimately, the European approach to privacy issues in terms of data is based on the protection of the individual as the most fundamental parameter.

This general conclusion obviously also includes satellite remote sensing data, whether under the European Convention on Human Rights or in the framework of EC law. Of particular interest in this respect is the GMES/Kopernikus initiative, which is to be not only a(nother) flagship of European cooperation in space, with the Commission as the political driving factor and ESA as the technical coordinator, but may also give rise to an enormous boost of satellite data and related activities downstream, as regards a variety of applications

[90] Cf. Art. 6(1), in particular (2), *Treaty on European Union*; also e.g. R.P. Folsom, *Principles of European Union Law*, (St. Paul: Thomson West, 2005) 57-59.

and services. In this sense, GMES/Kopernikus may well act as a catalyst also for increasing private activities at the level of generation of data by satellites, further to greater involvement in the downstream areas. If VHR satellite data are, indeed, going to be a major element in this development, then ever more privacy issues will rear their heads, whether at the individual or at the company level.

What does the above analysis, finally, mean for Athos and our German businessman? At this point in time, the international freedom to undertake satellite remote sensing activities, which was at the basis of the latter's interest, is (still) relatively undisputed. However, with the increasing advent of VHR satellite data on the scene, especially as part of the broader context of Google Earth's adventures and (other) Geographical Information Systems, it cannot be excluded that also on the international level consensus would increasingly be called for by at least some major stakeholders that the unfettered usage of space-borne data should be curbed. And whilst on the larger political level limitations to freedom of information-gathering will continue to be strongly resisted by the major space-faring nations, when it comes to the privacy of individuals and companies the outcome of such a discussion might not be a foregone conclusion.

At the other end, the Greek authorities will, for the time being, continue to be able to use their sovereign rights even within the context of EC law for the protection of the interests of Athos, as they did *vis-à-vis* the German businessman. The current exceptions to the application of unfettered free-commerce regulations, within the current set of relevant EC instruments, leave ample room for that. Indeed, as long as the Greek authorities refrain from discrimination in allowing a local businessman to do what the German one was not allowed to do, there is little chance this would change.

The only option left to the German businessman, therefore, would be to offer his satellite pictures to those interested who are outside the reach of Greek sovereign jurisdiction. Nevertheless, it would be prudent of him to ensure that any authorities dealing with such a matter would not support the Greek view and uphold relevant obstacles within their jurisdiction as well. Whether that leaves enough of a business case to be still of interest to him is another matter; any potential intrusion into the holy atmosphere at Athos will be removed far enough from the scene itself to justify limiting the internationally recognized freedom of information gathering for the purpose.

Even though such an outcome is the result of a perhaps an unnecessarily complicated construction – the alignment of two European approaches, on top of the international and national regimes relevant for privacy issues stemming from the usage of VHR satellite data – it does reflect the general European attitude that a fair balance has to be struck between commercial opportunities and the individual's rights to privacy. In other words, the alignment of these two European approaches has caused the international regime, which enshrines the freedom of space activities such as information gathering by satellite, to meet any given particular national regime in the middle. National sovereignty it therefore utilized for the purpose of preserving 'privacy'.