

IAC-14-E3,5-E7.6

PRIVACY, EARTH OBSERVATIONS AND LEGAL WAYS TO RECONCILE THE TWO

Catherine Doldirina, Dr.

Joint Research Centre, Italy, kdoldirina@yahoo.com

Development of the sensors used for Earth observation activities has been dramatic since the inception of these activities back in 1960s. Today the technology allows generation of very high resolution data and images with 50cm² resolution can be routinely purchased today on the commercial market. Satellite Earth observation data are used for a variety of applications ranging from emergency response and humanitarian operations, agriculture and mining, through to various forms of monitoring and military purposes.

The concept of privacy, including its legal dimension, remains vital in many societies. Privacy concerns and their protection are necessarily addressed by regulations in many jurisdictions. However, the understanding of what privacy is, what and to what extend it protects, is not uniform. This has implications on the conduct of a number activities, including services available over the internet, and potentially satellite Earth observation activities.

The ever increasing capabilities of satellite Earth observation technologies and their impact on the protection of privacy need to be reconciled. The analysis of this exercise is conducted from the perspective of different understanding of privacy in various jurisdictions on the one hand, and transborder nature of space activities on the other. In addition, it explores legal solutions to the situations where satellite Earth observation data are combined with other data and incorporated in geographic information systems that allow generation of new links between various information sources that if used may affect privacy. Usefulness of satellite Earth observation data for various purposes and activities, the necessity to foster further development of satellite Earth observation technologies, as well as their 'private' dimension – engagement of private companies – is taken into account to adequately address these issues.

I. INTRODUCTION

Development of new technologies and of the policy and regulatory regimes applicable to their use affect prioritisation, protection and balance of various interests. Within the domain of satellite Earth observation (remote sensing) activities, advances in the sensor technologies, the number of operational satellites that generate data, as well as the number and diversity of applications for which the data can be used has led to several important outcomes. On the one hand, the governments enabled and now encourage commercial (and private) industry to take over or at least to participate more actively in satellite Earth observation activities, both in the upstream (hardware, satellite operations) and downstream (data dissemination, processing, production of information products and applications, delivery of information services) relevant markets. On the other hand, satellite Earth observation data produced or funded by governments more often are considered to be a public good and open access to them and their unrestricted use are encouraged in many jurisdictions. This leads to the growing acceptance of the principles of free, full and open data sharing as a default mechanism for many activities that utilise satellite Earth observation data.

However diverse the highlighted interests are, their strengthening and increased protection leads to availability of more data, the ability for wider

communities to acquire or otherwise access and use them, and increased production of information that serves various purposes and enables conduct of many different activities. In themselves these trends, and protection of the interest of many to have broader access to more data and information resources, are of course a positive development. Promotion of free, full and open access to and use of satellite Earth observation data aids, for instance, achievement of various societal benefits, like better environment, faster and more efficient response to emergency situations, or more sustainable management of natural resources.¹ However, there is always the other side of the coin.

There are a number of legitimate interests that also require protection, the essence of which is to limit access to data and restrict their use. Examples include various relevant obligations under public international law, national security interests, or intellectual property rights. The focus of the analysis within this paper is the interest of protecting one's privacy. Privacy represents a very important institute within any democratic society and is a recognised right of each individual that can be described as a sphere of a person's life that should be free from 'invasion' by any third party.²

This paper provides a brief sketch of the main characteristics of satellite Earth observation activities and data, as well as contains an overview of approaches to defining the concept of privacy. The two form the

basis for the assessment as to where the clash between privacy and satellite Earth observation activities lies, and how it can be remedied if at all. The analysis also includes some case law and good practices that help safeguarding privacy interests while enabling maximum sharing and reuse of satellite Earth observation data possible. Parallels to some other fields of transborder activities (like those on the internet) that pose challenges to successful implementation of regulations addressing privacy are brought up whenever they may assist the clarity and arguments of the analysis conducted.

II. EARTH OBSERVATION ACTIVITIES

Satellite Earth observation activities focus on operation of special satellites, the sensors of which are capable of remotely sensing the surface and the depths of the Earth and to generate data that describe their various properties. Earth observation satellites use active and passive sensors to generate the data: the latter operate like a photographic camera, while the former carry their own source of illumination (like radar sensors) and can “see through” things.

The chain of activities that result in generation of satellite Earth observation data includes the following steps: sending of a command with the coordinates of the location to be sensed to the satellite by the operator; acquisition of primary data by the satellite while passing over the designated location; initial processing of the acquired data aboard the satellite; transmission of the data to a receiving station; further processing, archival, making data available.

Satellite Earth observation technologies continuously advance and hence increase capacity of satellites to generate data of better quality, different wavelength, spatial and temporal resolution, while sophisticated processing techniques³ enable production of customer- or application-tailored information services and products. This has contributed to the increase of situations where satellite Earth observation data and information are indispensable for successful conduct of various economic, research, governance and other activities. For instance today, monitoring, measuring and understanding Earth environment and its interaction with human activities⁴ are virtually impossible without satellite Earth observation.

Satellites are capable of generating views of the entire planet, without the constraints imposed by political or geographical frontiers. The unique features of many Earth observation satellites make products made from data they generate also unique and leads to world-wide data distribution and expansion of the relevant markets.⁵ Traditional use of satellite Earth observation data for environmental research has largely expanded in recent years. Companies that process

satellite Earth observation data deliver services for such economic activities and businesses as mapping, forestry, mining, agriculture, urban planning, news-making, shipping, real-estate, geographic information systems (GIS) and many others.⁶ They are also beneficial in different spheres of public activities, like health care, sustainable use of energy resources, decision-making at all government levels, cadastre maintenance, disaster relief and rescue operations to name just a few. Due to such usefulness of satellite Earth observation data access to them, whether as a public good⁷ or a commercially available product, has increased.

These developments result in participation in satellite Earth observation activities of many more actors, be it private companies or governments.⁸ The inevitable outcome of such increase participation is the necessity to protect the interests behind it. For governments it can be making satellite Earth observation data available to various communities of users, while for commercial companies it usually is protection of their business interests, market positions and outreach. However diverse these interests are, they may interfere with and potentially need to be balanced against other interests, including the right of privacy.⁹

III. PROTECTION OF PRIVACY

III.I Regulatory framework

Privacy is considered a human right, and is regulated both internationally and on the national level. It's codified in such sources of international law as the United Nations Declaration on Human Rights,¹⁰ International Covenant on Civil and Political Rights,¹¹ European Convention on Human Rights,¹² and American Convention on Human Rights.¹³

National policies and statutes are quite numerous. For examples, the United States has a Privacy Act of 1974¹⁴ that however only regulates collection of records by federal agencies that information identifying an individual.¹⁵ In addition, there are some federal¹⁶ and state data protection laws. The legislation of the United States is often critiqued for being sectoral and not systematic.¹⁷ At the European level, there is an overarching legal framework established by the European Union complemented and further detailed by the national legislation of its Member States. The legal instruments of the European Union are the Directive on protection of personal data¹⁸ that is currently under reform,¹⁹ and the E-Directive on privacy and electronic communication.²⁰ Transformation of the norms contained in both Directives aims at harmonisation of the legislation in the Member States.²¹ Certainly national privacy and data protection legislation is not limited to these two jurisdictions: many other countries have enacted relevant regulatory acts.²² They are not

addressed or otherwise referred to in order to avoid complicating the analysis.

III.II Definition

The essence of the right to privacy in the wording of the UN Declaration on Human Rights is that “no one shall be subjected to *arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation*” (emphasis added). This right is therefore a negative right,²³ but since it does not exist in the vacuum it needs to be balanced against other negative rights and freedoms. The term ‘balance’ is quite central to this topic and is referred to throughout the analysis. Definitions in many other international and domestic regulatory sources are often modelled on the one highlighted, but in addition they normally establish the basis for striking a balance between privacy and other interests. For instance, Article 8 of the European Convention on Human Rights provides that privacy can be interfered with if it is done by a public authority in accordance with the law and necessary in a democratic society in the interests of: national security, public safety or the economic wellbeing 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.

If one looks closely, neither the cited basic definition in the UN Declaration, nor the added mechanism to restrict the right contain a clear explanation as to what the actual meaning of privacy is. Absence of a precise definition is characteristic of privacy.²⁴ The addition of the basis to interfere with privacy often makes the definition of privacy a responsibility of the courts that deal with it in context of each individual case presented to them.²⁵

At the same time, determination of at least the approach as to how to define privacy is important, particularly taking into account 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. Many researchers agree that provision or codification of a precise definition of privacy is an impossible task,²⁶ and that despite its importance to society it remains a very vague concept.²⁷ Privacy is regarded to encompass such notions as non-interference with family, home or correspondence, freedom of thought, control over one’s body and personal information, freedom from surveillance, and protection from searches and interrogations.²⁸

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. Some of the most common approaches can be divided in five categories.²⁹ The first

one understands privacy as being let alone or the right of personality with the ability of an individual to determine the extent of the communication of personal information about oneself to others.³⁰ The second links privacy to sexual autonomy or intimacy³¹ and stipulates that privacy as essential for human relationships.³² The third category associates privacy with the control of information about oneself:³³ it primarily focuses on the ability to selectively disclose³⁴ information regarding privacy issues. The fourth emphasises the focus of privacy to enable control 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 “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”³⁵ that “entitles one to exclude others from watching, utilising, invading his private realm.”³⁶ The fifth brings forward the notion of the ability to limit access to oneself.³⁷

Any precise definition of what privacy, most often given in courts, will largely depend on its understanding in a specific jurisdiction and culture of public and private spheres of life, of public and private geographical places, as well as of public and private information. It will likely also depend on the accessibility of information to the unenhanced senses, and on the actual state of the knowledge within a given society.

The emerged concept of ‘data protection’ or ‘personal data’ poses today an additional difficulty. It can be confused with privacy, but is deemed to be a broader concept that encompasses any information (not only of private or personal character) that can be used to identify individuals.³⁸ For instance, the EU Data Protection Directive regulates handling of information obtained, stored, processed or supplied that relates to living individuals who could be identified by it (as opposed to protection of information related to privacy). Case law of the European Commission on Human Rights,³⁹ of the European Court on Human Rights,⁴⁰ and of the European Court of Justice⁴¹ also highlights this distinction.

To summarise, the concept of privacy, while directed at the protection of one’s personal life and reputation, family, home and correspondence, is not easy to define precisely. In addition, in some jurisdictions the range of data or information that may fall under the scope of regulatory protection is very wide. Last but not least, the regulatory systems enacted to protect privacy or processing of personal data in various countries are different.⁴² These factors, in particular when taken together, may represent the foundation for the inconsistencies in protecting interests of those pursuing satellite Earth observations activities and of those wishing to safeguard their privacy.

IV. CLASH OF INTERESTS

There is very little doubt as to whether development of new technologies, especially those that enable surveillance or communication of data (which include at least some technology related to space activities, like satellite Earth observation) may negatively affect privacy. In the sphere of space activities privacy was identified as an issue to be affected and addressed as early as in the seventies.⁴³ Privacy maybe a significant issue for satellite Earth observation activities where data and information they generate reveal personal information about identifiable individuals.⁴⁴

More and better technological capabilities reduce the costs of data collection, which has led to the situation of accumulation of too much (sometimes unnecessary) data. Some researchers fear that development of technology may lead to acceptance of more or different interferences with privacy by either individuals or courts,⁴⁵ and result in protection available only when the right of privacy is actively violated.

The ways data are stored and accessed nowadays, for example as in the case of interactive maps that integrate various types of data, including satellite Earth observation data, into GIS, may result in wider availability of private or personal information available to the public. Zooming function available when browsing GIS with specific queries may make available personal or other information linked to a specific geographic location or even an individual.

The fact that data are easily transmitted and used across borders is of particular relevance to Earth observation data, geographic data in general and GIS.⁴⁶ Existing differences regarding regulatory framework for privacy protection, its interpretation and implementation across jurisdictions potentially make finding the right balance between privacy and technology particularly difficult.

In this context, organisations engaged in satellite Earth observation activities must consider a number of legal risks when generating, collecting, processing, using or transferring geospatial data, one particular risk being that of violating an individual's right to privacy. Failure to avoid violations may result in suspension or termination of the data generation or processing activity, as well as in imposition of monetary damages and other types of liability.⁴⁷ Data providers, particularly when acting internationally, must ensure that their data do not contravene international or national regulatory sources for privacy protection, for instance by taking steps to remove, aggregate, anonymise or summarise confidential data.⁴⁸

Privacy interests can be affected and their accommodation should be addressed at different phases or aspects of satellite Earth observation activities. These

stages, as well as some ideas as to what should be done are highlighted here.

The actors who plan to carry out commercial satellite Earth observation activities, in particular by operating satellite systems, usually (depending on the laws of their domestic jurisdiction) need to acquire a licence that enables them. A licence is the result of an approval or authorisation process that is set up by the relevant regulations within the state where it is sought. The requirements that need to be satisfied in order to be granted the licence may include those related to privacy, especially what regards secure transmission of data from the satellite to the receiving ground station, as well as with regard to restrictions that may be imposed on dissemination of acquired data (by persons or territories). Thereby some aspects that serve the purpose of balancing the interest of carrying out commercial satellite Earth observation activities and of the protection of privacy may be addressed already at the very inception or even at the planning stage of these activities.

Another instance where the observation and privacy interests may clash is the phase of data generation or collection. The issue here may be centred on the need to exercise control in order to assess whether data should be gathered in the first place. The necessity to make such decisions rapidly and particularities with regard to ordering Earth observation data and satellite tasking make assessment of the balance between different interests difficult during this phase. Due to these practical circumstances such decisions probably should be made *ex post* rather than *ex ante* the data are generated.

The next phase – of data processing – will most likely reveal with sufficient degree of certainty whether privacy interests can be affected in each specific case. The more sophisticated processing is, and the more knowledge the data processor has with regard to the purpose of products' use, the better his position is to decide whether special attention to privacy interests needs to be paid. Regulatory framework regarding privacy protection should provide guidance as to what decisions should be made and what mechanisms can effectively be used not to jeopardise interests related to privacy.

The phase of data integration – integration of satellite Earth observation data with data from other sources and types, as well as into data and information systems – is the one that has the greatest potential of affecting privacy interests. The process of integration is significant to the extent that it can make otherwise neutral data reveal personal or private information that may prevent them from circulation and dissemination. The issues involved in the data integration activity do not necessarily relate to carrying out satellite Earth observation activities *stricto sensu*. They go beyond,

into the realm of producing and delivering information products and services and hence will be subject to regulatory regime applicable to these activities. Particular attention within this phase should be paid to legal issues pertaining to Big Data and legal implications of conducting transboundary activities, for example when making data available across or in different jurisdictions. The issues involved may be very complex for handling. A suggestion for those conducting satellite Earth observation activities but are not directly involved in the data integration activities is to ensure that the issues of responsibility and liability are properly addressed when data are licensed to those carrying out data integration activities.

Another issue, linked to responsibility and liability, concerns the actors who should or must ensure that privacy is not affected by at least introducing measures to reduce the risk of violating them. Taking into account the phases of satellite Earth observations activities as described above in this section, these can be different. The responsible actors include a satellite operator, a data provider or a data processor/integrator.

This brief overview of the phases of satellite Earth observation activities and their potential relation to privacy interests and their protection shows yet again how complex this field can potentially be and highlights, albeit very superficially, what can or should be done to avoid or reduce the risk of violating privacy once the activity is already taking place. Further safeguards that the law provides involved actors with are touched upon in the next section.

V. SAFEGUARDS

Potential or actual clash between the development of (satellite Earth observation) technology, use of applications it enables and privacy interests, as pointed out earlier, can be reconciled if or when the balance between the degree of accommodation of the various interests they represent is reached. Due to the unexpected (from the legal perspective) aspects of new technologies, as well as to the vague nature of the concept of privacy the correctness of the balance will depend upon circumstances of each particular case where such interests are at stake.

In order to reduce uncertainty in interpreting the concept and the principles of privacy protection, regulatory framework in various jurisdictions pertaining to the protection of privacy normally offers some procedural rules that aim at clarifying application of these principles. Privacy as a human right has to be reconciled against other interests and if this is done correctly, exceptions to its protection maybe successfully imposed. The regulatory framework contains guiding rules in accordance to which these exceptions can be applied.

Caution should be applied when exceptions or limitations to privacy protection principles are enforced. One of the primary mechanisms to effectively ensure their limited and only necessary application is a system of well-defined and detailed procedural rules that reduce the possibility of making biased or non-transparent decisions. Such rules should contain necessary elements that would guide decision making procedure with regard to limiting access to government data. For example, Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data and the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data require adherence to a set of rules, following which personal information must be:

- obtained fairly and lawfully;
- used only for the original specified purpose;
- adequate, relevant and not excessive to purpose;
- accurate and up to date; and
- destroyed after purpose for which it was obtained is completed.

These guiding rules may be criticised for being generic in the same fashion as the concept of privacy protection itself, as they still leave quite some room to interpretation and leverage in each particular case. In addition, they are not applied irrespective of other rules that protect other, often polar interests of equal or at least similar weight.

When one turns to other fields of law that govern protection of human rights, an interesting albeit worrisome observation can be discovered. For example the regulatory framework for access to government information (development of which was heavily driven by the recognition of the human right to form opinions and for this purpose to have access to information) also calls for restrictive interpretation of limitations to the right of access to government information. One of these limitations is protection of privacy. It is advisable that the following measures are taken into account to ensure restrictive application of the privacy limitation:⁴⁹

- treat protection of privacy as an exception to the general rule regarding widest access to government data that necessitates its narrow interpretation;
- verify that indeed privacy and integrity of the individual will be undermined if data are made available;
- make data available if privacy interests are or will not be affected.

The example highlighted serves the purpose of showing how in fact complex the task of balancing and adequately protecting various interests important to a society and its members is. This complexity often has a considerable impact on the decisions taken by various authorities responsible for either protection of privacy

or other competing interests, as well as case law. Broad categories of limitations, as well as vague character of the criteria of their implementation may pose difficulties in their straight forward and strict assessment by the institutions producing, holding the data, or other actors.

Whenever necessary, specific guidance as to interpretation of the notion of public interest should be provided through regulatory instruments or relevant case-law.⁵⁰ In the European Union a potentially far-reaching assessment of the relationship between disclosure of personal data and the economic interests of third parties was most recently done by the European Court of Justice in its judgement in Case C 131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.⁵¹ The Court in paragraph 81 points out the necessity of achieving “a fair balance” between the interest of the public to have access to information and the interest to protect the fundamental rights of privacy and protection of personal information based on the circumstances on the specific case at hand.⁵²

Another activity addressed by a number of courts concerns use of surveillance technologies, which satellite Earth observations maybe a part of, should also be taken into account. In the United States for a considerable period of time courts held that government agents could inspect individuals' homes without a warrant by using Forward Looking Infrared (FLIR) systems, or equivalent devices, to read and analyse the characteristics of invisible thermal infrared emissions⁵³ that could lead to detection of illegal or criminal activities. With the development of these practices, however, the balance of interests eventually shifted towards favouring protection of privacy, when courts started to prohibit a warrantless FLIR inspection of a private building as infringing privacy interests.⁵⁴

Implications of the use of imagery of the surface of the Earth and objects on it on privacy interests can be highlighted through the dispute between actress Barbra Streisand and Mr. Adelman. It focussed on the legitimacy of displaying a photograph of her house on a website containing images of the entire California coastline and highlight overdevelopment.⁵⁵ In this case the court adjudicated that the environmental purpose of the use of photographs on the website did in fact override privacy interests of the owners of the houses built along the coastline.⁵⁶

V. CONCLUSION

Complex activities composed of many different aspects, phases of which can be carried out by various

actors independent from each other require complex regulatory regimes to adequately govern them. Non-availability of straightforward and clear guidelines for making necessary decisions may be seen as a hurdle to development of certain activities. However, the degree of flexibility it may offer can in fact be more adaptable to an evolving activity than a rigid and detailed regulatory regime. Flexibility should in fact be always present, as too much rigidity can stifle progress in satellite Earth observation activities, or jeopardise mechanisms in place to protect privacy.

Advancement of space technology in general and of satellite Earth observation technology in particular will inevitably have implications on privacy and its protection. The very nature of the sensors of Earth observation satellites – their ability to see things on the surface of the Earth and beyond – may lead to discovery of information that should remain private. Due to this characteristic feature satellite Earth observation activities fall under the regulatory framework addressing protection of privacy and need to be compliant with it.

Resolution of potential or actual violations of privacy may not be an easy task because even the legal definition of the concept of privacy is often missing from the regulations governing its protection. This leaves room for interpretation of the norms of the applicable regulatory regimes to actors who conduct satellite Earth observation activities, to government authorities who supervise them, as well as to courts that resolve arising disputes involving privacy. Such a situation may result in inconsistencies in interpretation and application of the regulatory regimes in force.

The highlighted phases of where specifically privacy interests can be affected and hence need to be addressed, could be used in planning and procedurally arranging satellite Earth observation activities. For example, certain requirements regarding protection of privacy interests can be incorporated in the licence for those planning to conduct these activities on the commercial basis. Furthermore, whenever a subject of an activity is changed (for example from a satellite operator to a data processor or integrator) liability and responsibility should be transferred from one to the other in order to avoid multiplicity of actors that can be complained against.

The situation with satellite Earth observation activities, however, is not unique and developments and practices with regard to reconciling interests behind other, similar technologies and privacy maybe useful for addressing specific concerns in this particular field of activities.

¹ See GEOSS 10-Year Implementation Plan at p.27. 2003 GEO Washington Summit. Online: [http://earthobservations.org/docs/GEOSS%2010-Year%20Implementation%20Plan%20\(GEO%201000\).pdf](http://earthobservations.org/docs/GEOSS%2010-Year%20Implementation%20Plan%20(GEO%201000).pdf).

² See Littman, M. & Carter-Ruck, P., *Privacy and the Law: A Report by Justice* (London: Stevens & Sons Ltd, 1970), at 5.

³ See e.g. Uttenthaler, A. & Barner, F., Euro-Maps 3D – An Innovative Elevation Dataset for Various Applications. *e-GEOS International Conference* (Rome, May 22-24, 2012), online: <http://www.e-geos.it/news/meeting12/presentations/23-Uttenthaler-Euromap.pdf>; Passini, G., 3D Geospatial. *e-GEOS International Conference* (Rome, May 22-24, 2012), online: http://www.e-geos.it/news/meeting12/presentations/21-Passini_e-GEOS.pdf.

⁴ Tatem, A.J., Goetz, S.J. & Hay, S.I. “Fifty Years of Earth-Observation Satellites” (2008) 96:5 *American Scientist* 390.

⁵ *The Cambridge Encyclopaedia of Space: Missions, Applications and Exploration* (Cambridge, New York: Cambridge University Press, 2003) at 4.

⁶ Campbell, G., New Business Relations for EO. *e-GEOS International Conference* (Rome, May 22-24, 2012), online: <http://www.e-geos.it/news/meeting12/presentations/04-Campbell-ESA.pdf>.

⁷ Milinski, M. *et al.* “Stabilizing the Earth’s Climate is not a Losing Game: Supporting Evidence from Public Goods Experiments” (2006) 103:11 *Proceedings of the National Academy of Sciences of the United States of America* at 3994.

⁸ See an interesting overview of the expenditure for civil space programmes and satellite Earth observation activities in Keith, A., Emerging Space Programs Spark Earth Observation Growth. *Earth Imaging Journal* (2014), online: <http://ejournal.com/2014/emerging-space-programs-spark-earth-observation-growth#sthash.a5How8SR.dpuf>. See also Revillon, P., Earth Observation Market Evolution and Drivers. *e-GEOS International Conference* (Rome, May 22-24, 2012), online: <http://www.e-geos.it/news/meeting12/presentations/24-Re%81Lvillon-Euroconsult.pdf>.

⁹ For considerations regarding impact of the development of satellite Earth observation technologies on such spheres as economy, national security and privacy see Hitchings, S., Policy Assessment of the Impacts of Remote-sensing Technology. *Space Policy* 19 (2003), 119-125.

¹⁰ Article 12 United Nations Declaration on Human Rights, 10 December 1948, 217 A (III).

¹¹ Article 17 International Covenant on Civil and Political Rights. 999 *U.N.T.S.* 171.

¹² Article 8 European Convention on Human Rights. 213 *U.N.T.S.* 221. Note that the term ‘privacy’ is not used in the Convention.

¹³ Article 11 American Convention on Human Rights. 1144 *U.N.T.S.* 123. Other instruments include Cairo Declaration on Human Rights in Islam, August 5, 1990, *U.N. GAOR*, World Conf. on Hum. Rts., 4th Sess., Agenda Item 5, U.N. Doc. A/CONF.157/PC/62/Add.18 (1993) [English translation]; Declaration of Principles on Freedom of Expression in Africa, African Commission on Human and Peoples' Rights, 32nd Session, 17-23 October, 2002, online: <http://www1.umn.edu/humanrts/achpr/expressionfreedomdec.html>; Council of Europe Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows 11 August 2001. *E.T.S.* 181; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. 11 July 2013 C(2013)79.

¹⁴ Privacy Act, 31 December 1974. 5 *U.S.C.* § 552a.

¹⁵ Information available online: <http://foia.state.gov/Learn/PrivacyAct.aspx>.

¹⁶ The Health Insurance Portability and Accountability Act, 21 August 1996, Pub.L. 104–191, 110 Stat. 1936; The Fair and Accurate Credit Transactions Act, 22 November 2003, Pub.L. 108–159; Children’s Online Privacy Protection Act, 21 October 1998, 15 *U.S.C.* §§ 6501–6506.

¹⁷ See e.g. Cassini, J.A., Medlin B.D., Romaniello, A., Laws and Regulations Dealing with Information Security and Privacy: An Investigative Study. *International Journal of Information Security and Privacy* 2(2)(2008), 81; Dimov, D., Differences between the privacy laws in the EU and the US. Infosec Institute (2013), online: <http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/>.

¹⁸ Directive 95/46/EC of the European Parliament and of the Council 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. *OJ L* 281, 23/11/1995, 31-50.

¹⁹ Commission proposes a comprehensive reform of the data protection rules (25 January 2012), online: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

²⁰ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. *OJ L* 201, 31/07/2002, 37-47.

²¹ For a comprehensive overview of the regulatory regime in the European Union, its transformation by the Member States, differences from the regime established in the United States, as well as overview of some non-European countries' privacy legislation, see Dowling, D.C. Jr., *International Data Protection and Privacy Law*. White & Case (2009), online: http://www.whitecase.com/files/publication/367982f8-6dc9-478e-ab2f-5fdf2d96f84a/presentation/publicationattachment/30c48c85-a6c4-4c37-84bd-6a4851f87a77/article_intldataprotectionandprivacylaw_v5.pdf.

²² For an overview of the relevant regulatory mechanisms in 63 different jurisdictions see Data Protection Laws of the World. DLA Piper (2013), online: http://files.dlapiper.com/files/Uploads/Documents/Data_Protection_Laws_of_the_World_2013.pdf.

²³ Sofsky, W. *Privacy: A Manifesto*. Rendall. S transl. (Princeton University Press, 2008), at 30.

²⁴ Michael, J., *Privacy and Human Rights* (UNESCO 1994) at 1.

²⁵ See generally Hart Ely, J., The Wages of Crying Wolf: A Comment on *Roe v. Wade*. *Yale Law Journal* 82 (1973), 920-49.

²⁶ Schoeman, F., *Privacy and Social Freedom* (1994), 11-23; Posner, R., The Right of Privacy. *Georgia Law Review* 12 (1978), 401 For a philosophic discussion of defining privacy see Power, M., A Cognitive Access Definition of Privacy. *Law and Philosophy* 15 (1996), 369-386.

²⁷ Samar, V. J., *The Right to Privacy* (Philadelphia: Temple University Press, 1991), 13; Thomson, J. J., The right to privacy, *Philosophy and Public Affairs* 4(4) (1975), 295.

²⁸ Solove, D.J. *Understanding Privacy* (Harvard University Press, Cambridge: 2008); Sloot, v.d. B., Privacy in the Post-NSA Era: Time for a Fundamental Revision? *JIPITEC* 5(2014), section C; Aquilina, K., Public Security vs Privacy in Technology Law: A Balancing Act? *Computer Law and Security Review* 26 (2010), section 2.5.

²⁹ Parent, W. A., Recent work on the concept of privacy. *American Philosophical Quarterly* 20(4) (1983), 341-355.

³⁰ Warren, S & Brandeis, L. The Right to Privacy 4 *Harvard Law Review* 193(1890).

³¹ Inness, J. *Privacy, Intimacy and Isolation* (New York: Oxford University Press, 1992), 73.

³² With the problem that some private things, like bank account information, are private but not intimate

³³ Fried. Privacy, in *Law, Reason, and Justice: Essays in Legal Philosophy* (Graham B. J. Hughes ed., 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

³⁴ Karst, K.L. The Files': Legal Controls over the Accuracy and Accessibility of Stored Personal Data. 31 *Law and Contemporary Problems* 342 (1966), 344.

³⁵ Godkin, E.L. Libel and Its Legal Remedy. 12 *Journal of Social Science* 69 (1880), 80.

³⁶ Van Den Haag, E. On Privacy, in *Nomos XIII: Privacy* 149 (J. Roland Penncock & J.W Chapman eds. 1971).

³⁷ Gavison, R., Privacy and the limits of law. *The Yale Law Journal* 89(3) (1980), 428. See also Doldirina, C., What is Privacy? in *Current Legal Issues for Satellite Earth Observation*, ESPI Report (2010), 50-55.

³⁸ Sloot, v.d. B., Privacy in the Post-NSA Era: Time for a Fundamental Revision? *JIPITEC* 5 (2014), 6.

³⁹ See e.g. *Murray v. Great Britain* 14310/88, 10 December 1991; *Herbecq v. Belgium* 32200/96, 32201/96, 14 January 1998.

⁴⁰ See e.g. *Copland v. United Kingdom* 62617/00, 3 April 2007; *Segerstedt-Wiberg and Others v. Sweden* 62332/00, 6 June 2006.

⁴¹ See e.g., *Tietosuoja valtuutettu [Finnish data protection ombudsman] v. Satakunnan Markkinaporssi Oy and Satamedia Oy* C-73/07, 16 December 2008. See also Laudati, L., EU court decisions relating to data protection (2012), online: http://ec.europa.eu/anti_fraud/documents/data-protection/dpo/ecj_decisions_relating_data_protection_en.pdf.

⁴² See an interesting discussion on different privacy regulation and business activities in Private data, public rules. *The Economist* (28 January 2012), online: <http://www.economist.com/node/21543489>.

⁴³ Legal Aspects of the Privatisation and Commercialisation of Space Activities, Space Law Committee Fifth and Final Report, International Law Association, Sofia Conference (2012), at 6, online: https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0CD4QFjAE&url=http%3A%2F%2Fwww.ila-hq.org%2Fdownload.cfm%2Fdocid%2F4F84FC9C-9ECF-4D3F-A697ABE442A3BFE6&ei=z_8OVMKVO4GyPP37gdAD&usq=AFQjCNHHNr4BnDZHQYhAnvYHpolkH6z7CA&bvm=bv.74649129,d.ZWU. See also First Report on Dispute Settlement, Suborbital Flights, Use of Satellite Data

and Space Debris, Space Law Committee, International Law Association, Washington Conference (2014), Section 3, online: <http://www.ila-hq.org/download.cfm/docid/0A542400-50F8-4E98-85F82E0F8DCA2631>.

⁴⁴ London Institute of Space Policy and Law, Evidence from Space, study for the European Space Agency (1012), at 40, online: http://www.space-institute.org/app/uploads/1342722048_Evidence_from_Space_25_June_2012_-_No_Cover_zip.pdf.

⁴⁵ Gutterman, M., A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance, 39 *SYRACUSE L. REV.* 647 (1988), 650.

⁴⁶ Legal Aspects of the Privatisation and Commercialisation of Space Activities, Space Law Committee Fifth and Final Report, International Law Association, Sofia Conference (2012), at 6, online: https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0CD4QFjAE&url=http%3A%2F%2Fwww.ila-hq.org%2Fdownload.cfm%2Fdocid%2F4F84FC9C-9ECF-4D3F-A697ABE442A3BFE6&ei=z_8OVMKVO4GyPP37gdAD&usq=AFQjCNHHNr4BnDZHQYhAnvYHpolkH6z7CA&bvm=bv.74649129,d.ZWU. See also First Report on Dispute Settlement, Suborbital Flights, Use of Satellite Data and Space Debris, Space Law Committee, International Law Association, Washington Conference (2014), Section 3, online: <http://www.ila-hq.org/download.cfm/docid/0A542400-50F8-4E98-85F82E0F8DCA2631>.

⁴⁷ Liability Issues in the Global Earth Observation System of Systems, Legal Liability Sub-Group, Data Sharing Task Force, Group on Earth Observation, online: https://www.google.it/url?sa=t&rct=j&q=&esrc=s&source=web&cd=9&cad=rja&uact=8&ved=0CFsQFjAI&url=http%3A%2F%2Fsites.nationalacademies.org%2FPGA%2Fcs%2Fgroups%2Fpgasite%2Fdocuments%2Fwebpage%2Fpga_063052.doc&ei=z_8OVMKVO4GyPP37gdAD&usq=AFQjCNG87H_ZhihtJghU9JteGBGf6AX43w&bvm=bv.74649129,d.ZWU.

⁴⁸ Liability Issues in the Global Earth Observation System of Systems, Legal Liability Sub-Group, Data Sharing Task Force, Group on Earth Observation.

⁴⁹ Kierkegaard, S., Open access to public documents – More secrecy, less transparency! *Computer Law & Security Review*, 25:1 (2009), 3-27.

⁵⁰ Moravcsik, A. & Sangiovanni, A., On democracy and "public interest" in the European Union. *Center for European Studies working paper series* 93 (2003), 122-148.

⁵¹ Case C-131/12, online: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=32612>.

⁵² European Commission, Factsheet on the "Right to be Forgotten" ruling (C-131-12), online: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

⁵³ United States v. Domitrovich, No. CR-93-295-FVS, 1994 U.S. Dist. LEXIS 6928 (E.D. Wash. Mar. 24, 1994); United States v. Porco, 842 F. Supp. 1393 (D. Wyo. 1994); United States v. Kyilo, 809 F. Supp. 787 (D. Or. 1992), remanded for evidentiary hr'g, 37 F.3d 526 (9th Cir, 1994); United States v. Deaner, No. CR-92-0090-01, 1992 U.S. Dist. LEXIS 13046 (M.D. Pa. July 27, 1992), affd on other grounds, 1 F.3d 192 (3d Cir. 1993); United States v. Penny-Feeney, 773 F. Supp. 220 (D. Haw. 1991), affd on other grounds, 984 F.2d 1053 (9th Cir. 1993). Referred to in Susan Moore, Does Heat Emanate Beyond the Threshold - Home Infrared Emissions, Remote Sensing, and the Fourth Amendment Threshold, 70 *Chi.-Kent. L. Rev.* 803 (1994), at 807.

⁵⁴ United States v. Ishmael, 843 F. Supp. 205 (E.D. Tex. 1994) (order granting defendants' motion to suppress), rev'd, No. 94-40159, 1995 U.S. App. LEXIS 4957 (5th Cir. Mar. 15, 1995); see also, United States v. Field, No. 94-CR-0013-C, 1994 U.S. Dist. LEXIS 8829 (W.D. Wis. June 9, 1994) (holding that thermal imaging of a residence constitutes a Fourth Amendment search.). Washington v. Young, 867 P.2d 593 (Wash. 1994). The Washington constitution protects an individual's home and "private affairs" from warrantless searches. *Id.* at 597 (referring to WASH. CONsT. art. 1, § 7). In Moore, *id.*

⁵⁵ Barbra Streisand vs. Kenneth Adelman, Case No.SC077257, decision December 31, 2003, online: <http://www.californiacoastline.org/streisand/slapp-ruling.pdf>

⁵⁶ Maria Alicia Gaura, Judge tosses Streisand's suit to keep estate photos off Web. She argued activist's aerial shots invaded her privacy. *San Francisco Gate*, December 4, 2003, online: <http://www.sfgate.com/news/article/Judge-tosses-Streisand-s-suit-to-keep-estate-2525591.php>. See case history online: <http://www.californiacoastline.org/streisand/lawsuit.html>; see also Rene Millman, Google's right to be forgotten creates Streisand effect, *Recombu*, July 3, 2014, online: <http://recombu.com/digital/news/google-creates-streisand-effect-bbc-mail-guardian>.