Remote Sensing and the New European General Data Protection Regulation

*Brendan Cohen**

Abstract

The new European General Data Protection Regulation, which goes into effect in May 2018, will have a dramatic effect on companies, both within the EU and outside, that control or process personal data. In light of both the expanded territorial reach and the broader definition of personal information, companies that collect or process high resolution satellite images will likely need to ensure they comply with the new regulations. Given the more onerous obligations and the significantly increased penalties for failure to comply, companies must begin to ensure they are putting the proper procedures and tools in place now, so that they can be ready by May.

This paper also considers data protection issues related to the use of remote sensing to track migrants and refugees. While there are many beneficial uses of high resolution satellite images for their protection, the fact that these are such vulnerable populations means it is all the more important to ensure there is a balance and that the right to privacy is weighed against other fundamental rights like safety and security.

I. Introduction

In the three decades since the United States first commercialized satellite images from space under the LANDSAT program, earth observation satellites have improved dramatically. Currently, the highest resolution images that are commercially available are provided by DigitalGlobe's WorldView-3 and new WorldView-4 satellites, for which each pixel in a captured image corresponds to approximately 31 cm. While this is not yet sufficient to be able to distinguish an individual person, image resolution will only get better and is

* Cleary Gottlieb Steen & Hamilton LLP, United States, bcohen@cgsh.com. The opinions and views expressed herein are solely those of the author and do not necessarily represent those of Cleary Gottlieb Steen & Hamilton LLP or any of its clients.

certainly high enough today to discern details like cars and, as DigitalGlobe advertises, "manholes and mailboxes."[1]

A new European General Data Protection Regulation[2] (the "GDPR") was adopted on April 27, 2016 and will take effect on May 25, 2018. Under this regime, "personal data" is broadly defined and includes any information relating to a person who can be directly or indirectly identified in particular by reference to other data. Any entity that, directly or indirectly, collects or processes data of European Union residents is subject to the terms of the GDPR.

Even if it is not yet possible to directly identify an individual using today's satellites, commercial satellite companies arguably capture enough information to be able to indirectly identify an individual by reference to other imaged information. Since a non-EU entity is subject to the GDPR if it is monitoring a subject's behavior within the EU, any entity collecting or processing such data would arguably be subject to the requirements of the GDPR, even if the images are taken from a satellite under the jurisdiction and control of, and processed in, a non-EU country. This paper will examine the new regime that will be implemented by the GDPR and analyze its applicability to remote sensing applications.

II. Privacy Rights under Space Law

As an initial matter, any analysis of the activities of satellite operators must take into account the principles and regulations set forth in the *corpus juris spatialis*. It has been observed, however, that there is "an almost complete silence" in the space law treaties and resolutions with respect to private activities undertaken by non-state actors.[3] While Article VI of the Outer Space Treaty[4] requires States Parties to authorize, supervise and bear responsibility for the activities of non-governmental entities in outer space, such supervision appears to be limited to ensuring compliance by the private

1 *See US lifts restrictions on more detailed satellite images*, BBC, www.bbc.com/news/technology-27868703 (last visited Sept. 29, 2017).

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [hereinafter, GDPR].

3 Frans von der Dunk, *Sovereignty Versus Space – Public Law and Private Launch in the Asian Context*, 5 Singapore Journal of International & Comparative Law 22, 24 (2001), available at http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1000&context=spacelaw.

4 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, *opened for signature* Jan. 27, 1967, 18 U.S.T. 2410, T.I.A.S. 6347, 610 U.N.T.S. 205 [hereinafter, Outer Space Treaty].

actor with the provisions set forth in the Treaty. The Outer Space Treaty certainly does contain prohibitions and obligations on States Parties, and by extension, their nationals (for example, the non-appropriation principle in Article II and the liability obligations under Article VII), but there is no mention of privacy laws and much of the Treaty is designed to guarantee all states the freedom of exploration and peaceful use of outer space.[5]

The freedom to legally monitor the Earth from space is specifically embodied in the Remote Sensing Principles,[6] which, while not treaty law, have been adopted by consensus and are considered to reflect customary international law, binding on all states.[7] The Remote Sensing Principles contain no specific restrictions on what may be observed, give no veto rights to a sensed state or entity and put no operational conditions on the sensing (e.g., the image resolution that may be used).[8] With respect to privacy considerations, the Remote Sensing Principles do not provide any useful guidance. First, they are rather narrowly drafted and technically only govern States' "remote sensing" activities (defined as using electromagnetic waves to sense the Earth "for the purpose of improving natural resources management, land use and the protection of the environment"[9]). Although many commercial applications fit within these purposes, much of the data collected by today's satellite imaging companies go far beyond these three uses, making the Remote Sensing Principles inapplicable to most commercial applications. Furthermore, even though the Remote Sensing Principles reference Article VI of the Outer Space Treaty and reaffirm that States bear international responsibility for their remote sensing activities (regardless of whether such activities are actually carried out by non-governmental actors),[10] the focus of the Remote Sensing Principles are on the interests and rights of states to sense and be sensed, not on those of individuals. Thus, the Remote Sensing Principles are unlikely to provide much guidance with respect to an individual's rights under domestic laws vis à vis a commercial satellite operator.

---

5 *Id.* at art. I.

6 Principles Relating to Remote Sensing of the Earth from Outer Space. G.A. Res. 41/65, U.N. Doc. A/RES/41/65 (Dec. 3, 1986) [hereinafter, Remote Sensing Principles].

7 Atsuyo Ito, *Improvement to the Legal Regime for the Effective use of Satellite Remote Sensing Data for Disaster Management and Protection of the Environment*, 34 J. Space L. 45, 47 (2008) (citing Joanne Gabrynowicz, *Expanding Global Remote Sensing Services*, in PROC. WORKSHOP SPACE L. IN THE TWENTY-FIRST CENTURY 101 (2000)).

8 *Id.* at 49.

9 Remote Sensing Principles, *supra* note 6, at princ. I(a).

10 *Id.* at princ. XIV.

Another important source of space law is the Liability Convention,[11] which sets forth the allocation of liability resulting from damage "caused by a space object." Many authors have discussed the meaning of damage under the Liability Convention, but there is no clear answer as to whether indirect damages, such as harm resulting from a violation of one's privacy using a satellite, could result in compensable damages under the Convention. While the general view seems to be that such non-physical damages are not compensable,[12] there are arguments on both sides that will have to be tested or the language will have to be further clarified.[13]

Article III of the Outer Space Treaty makes it clear that the use of outer space must be done in accordance with international law, but since the right "to seek[], receive[] and impart[] information and ideas"[14] is fundamental under general international law, any limitations on the freedom to use outer space for the collection of space-based images should be based on domestic laws, applicable only within a state's territorial boundaries and to such state's nationals.[15] Thus, individual states are free to regulate, to the extent of their jurisdiction to enforce, national laws that govern the use of data collected from outer space in order to protect individual privacy.[16] One such regulation, which will be discussed in the following section is the new European GDPR.

---

11 Convention on International Liability for Damage Caused by Space Objects, *opened for signature* Mar. 29, 1972, 24 U.S.T. 2389, T.I.A.S. 7762, 961 U.N.T.S. 187 [hereinafter, Liability Convention].

12 *See* Stephen Gorove, *Some Thoughts on Liability for the Use of Data Acquired by Earth Resources Satellites*, 15 PROC. COLLOQ. L. OUTER SPACE 109, 109 (1972) (arguing that imaging data is not damage caused "by" the space object itself, rather it "result[s] from the intentional or negligent act of a party involving the use or dissemination of data"); *see also* Frans von der Dunk, *Outer Space Law Principles and Privacy*, *in* EVIDENCE FROM EARTH OBSERVATION SATELLITES, 241, 250 (Ray Purdy & Denise Leung, eds., 2012) (explaining the general consensus of commentators against the view that damages caused by the contents of a satellite fall within the regime of the Liability Convention).

13 *See* Elena Carpanelli & Brendan Cohen, *Interpreting "Damage Caused by Space Objects" Under the 1972 Liability Convention, in* 56 PROC. COLLOQ. L. OUTER SPACE 29, 38-39 (2013); von der Dunk, *supra* note 12, at 250 (citing B.D.K. HENAKU, THE LAW ON GLOBAL AIR NAVIGATION BY SATELLITE: A LEGAL ANALYSIS OF THE ICAO CNS/ATM SYSTEM 221 (1998)).

14 Universal Declaration of Human Rights, Article 19, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948); International Covenant on Civil and Political Rights, Article 19, *adopted* Dec. 16, 1966, 999 U.N.T.S 171 (entered into force Mar. 23, 1976).

15 Von der Dunk, *supra* note 12, at 247.

16 *Id.* at 248.

III. European General Data Protection Regulation

III. A Overview

Europe has long had strong data protection laws, but several years ago, the EU determined that the existing European data protection framework, established in 1995 by the Data Protection Directive ("DPD"),[17] was no longer sufficient to protect the fundamental rights of EU citizens in light of new technologies that have evolved in the last two decades. The GDPR, intended to be a comprehensive reform of data protection laws, will supersede the DPD. As a regulation, the GDPR will automatically be applicable in all EU Member States without requiring any enabling legislation.

While the new data protection regime provides increased safeguards for the privacy of individuals, it will result in a significantly higher burden on companies that will need to comply with the regulations. The remainder of this section describes certain of the provisions that may be applicable to commercial satellite operators, particularly those that collect and process high resolution satellite imagery.

III.B Subject Matter of the GDPR

The provisions of the GDPR apply to a company's use of "personal data." While many of the changes to the definition of personal data are intended to target operators of websites and others who collect data over the internet, the language of the regulation is intended to be broad enough to cover other forms of new technology. Thus, personal data includes not only what one would think of as traditional personal information (e.g., name, address, social security number), but also any information that can be used to identify a person directly or indirectly, whether on its own or when combined with another piece of information, including an image or location data of a person.[18]

Given the nature of the definition, it can be very difficult to determine whether certain data collected or held by a company would constitute personal data under the GDPR. However, the more disparate data is aggregated or combined with other data, the more likely it is that such data

17 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 [hereinafter, DPD].

18 Personal data means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR, *supra* note 2, at art. 4(1).

will be deemed personal. The recitals to the GDPR provide some guidance on the concept of identification:

> "To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used [by any person], such as singling out . . . to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."[19]

Conversely, the GDPR does *not* apply to anonymous data, that is data in which the data subject is not or no longer identifiable. The collection of statistical data without any link to an individual natural person thus falls outside the scope of the regulation.

III.C Territorial Scope

The GDPR also has a broader territorial reach than does the existing DPD. While both data privacy regimes apply to EU-based companies that control or process personal data,[20] the GDPR will also apply to non-EU based companies that control or process personal data of subjects who are in the EU, where the activities relate to the "monitoring" of their behavior within the EU.[21]

Whether the collection of satellite images would amount to monitoring, as used in this regulation, is not entirely clear. The recitals to the GDPR give an example of monitoring of data subjects, noting that one consideration is whether "natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes."[22] While this example is directed toward the use of online browsing activities, the purpose of the GDPR is ultimately meant to protect individual privacy and the use of personal data, protection of which is considered a fundamental right.[23] Thus, it is important to consider this context when determining whether a particular activity falls within the regime of the GDPR. Since high resolution satellite imagery coupled with ever-improving image recognition technology can allow a third party to determine a significant amount of information about an individual's location,

19 GDPR, *supra* note 2, at rec. 26.
20 DPD, *supra* note 17, at art. 4(1)(a); GDPR, *supra* note 2, at art. 3(1).
21 GDPR, *supra* note 2, at art. 3(2)(b).
22 *Id.* at rec. 24.
23 *Id.* at rec. 1 (citing Charter of Fundamental Rights of the European Union art. 8(1), 2000 and Treaty on the Functioning of the European Union (TFEU) art. 16(1), 2012).

activities and preferences, a strong case can be made that the collection and processing of such data could amount to monitoring under the GDPR.

The GDPR will continue to have restrictions on cross-border transfer of personal data that are similar to those restrictions that already apply under the DPD.[24] Such cross-border transfers are only allowed if the transfer is made to a jurisdiction that has been deemed by the European Commission to have an adequate level of data protection[25] or there is some other protection in place (e.g., through the implementation of model contractual clauses issued by the European Commission to ensure proper protection of personal data).[26] One interesting question this raises concerns the transfer of European personal data from a satellite under the jurisdiction and control of the United States to a data controller or processor located in the United States. Even if none of the ground stations that receive the data are physically located in Europe, a European data subject may have a credible argument that such transfer is subject to cross-border transfer restrictions. Going even further, even the initial collection of personal data from Europe using a U.S. satellite could be argued to constitutes a cross-border transfer.

In any event, under the new regime, even companies that have no presence in Europe now fall within the terms of the GDPR. This long-arm aspect of the GDPR could have a considerable effect on companies, since becoming compliant will likely be costly and involve significant preparation in advance of May 25, 2018.

III.D Obligations on Companies Subject to the GDPR

Another important concept under the GDPR concerns who processes personal data. As defined in the regulation, "processing" means any operations that are performed on personal data or sets thereof, "whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." The

24 Following a finding that the U.S. data protection rules were inadequate, and so EU data could not be transferred to the U.S., the U.S. and the EU agreed to a Safe Harbor Program in 2000. Under this program, U.S. companies could receive European personal data, provided they certify they have complied with processing standards that were equivalent to those required by the EU. In 2015 (*Maximillian Schrems v. Data Protection Commissioner*), the European Court of Justice determined the Safe Harbor Program to be invalid due to concerns that the U.S. intelligence agencies could access the data transferred from Europe. The U.S. and EU have since implemented a new data transfer protocol – the Privacy Shield Framework – that companies must comply with before transferring personal data to the U.S. from Europe.

25 GDPR, *supra* note 2, at arts. 44-45.

26 *Id.* at art. 46.

regulations apply to companies that serve as either data controllers or data processors. A data controller is the entity that "determines the purposes and means of the processing of personal data,"[27] while a processor "processes personal data on behalf of the controller."[28] Although these terms are largely unchanged from their definitions in the DPD, even companies that were previously subject to the DPD may have to consider their use of data now that the nature of the information subject to the GDPR in the first place is more expansive. While controllers bear the primary responsibility for compliance, processors are also now directly subject to the regulations[29] (this is in contrast to the DPD, where only controllers had direct legal compliance obligations[30]). The penalties for non-compliance include fines of up to the higher of (i) 4% of worldwide annual turnover (revenues) or €20 million for a breach of the requirements relating to international transfers of data or the basic principles for processing (such as conditions for consent) or (ii) 2% of worldwide annual turnover (revenues) or €10 million for a breach of other specified provisions, including many of the obligations of processors and controllers that are discussed below.[31]

If a company is subject to the GDPR because it controls or processes personal data and falls within the territorial scope of the regulation, the next question is, what must such company do to maintain compliance and avoid the fines discussed above? The obligations vary somewhat depending on whether the company is considered the controller or the processor, but both have direct obligations.

III.D.1 Controllers

As discussed above, data controllers are those entities that determine how personal data will be processed and for what purpose. Controllers bear the primary responsibility for ensuring compliance and must "implement appropriate and effective measures and be able to demonstrate the compliance of processing activities."[32] This principle of accountability, whereby companies must be able to demonstrate compliance, adds additional burdens.[33] Companies that are not processing sensitive personal data and have less than 250 employees are exempted,[34] but other controllers subject to the GDPR must keep records of any data processing activities, including the purposes of the processing, categories of data subjects, data recipients and

27 *Id.* at art. 4(7).
28 *Id.* at art. 4(8).
29 *Id.* at art. 3(1).
30 DPD, *supra* note 17, at art. 4(1).
31 GDPR, *supra* note 2, at art. 83.
32 *Id.* at rec. 74.
33 *Id.* at art. 5(2).
34 *Id.* at art. 30(5).

types of personal data, a description of data security measures taken and the controller's data retention policies.[35]

One related and important policy goal of the GDPR is to encourage companies to consider "data protection by design and by default." As described in the regulation, this is the concept that data protection should not be an afterthought – on the contrary, it is important to consider data protection during the design and development of any new products and services. A data controller must also implement appropriate technical measures ("taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing" as well as the risks to the data subject posed by the processing[36]) to make sure that only personal data that is necessary for a specific purpose is processed. Relatedly, the controller must ensure that, by default, personal data are not widely accessible "to an indefinite number of natural persons."[37]

Part of this requirement to take appropriate technical measures manifests itself in the data security obligations of data controllers. In order to mitigate any risk inherent in maintaining and processing personal data, controllers must take steps to prevent data from accidental or unlawful destruction, loss, alteration or unauthorized disclosure.[38] The GDPR gives certain examples of these measures, including encryption and backup of data, as well as regular testing of data security.[39] In the event of a data breach, a controller has an obligation to file a report with the applicable data protection supervisory authority ("DPA")[40] within 72 hours of its discovery of such a breach (unless such breach is not likely to harm the rights or freedoms of individuals whose data was breached).[41]

Depending on the nature of their activities, certain companies must now designate a Data Protection Officer ("DPO"). Of particular note here, a DPO is required where "the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale."[42] The Article 29 Data Protection Working Party (composed of representatives of the DPAs of each EU Member State and set up under the DPD to provide recommendations and advice regarding data protection matters) (the "Article 29 Working Party") analyzed the meaning of the terms

35 *Id.* at art. 30(1).
36 GDPR, *supra* note 2, at art. 25(1).
37 *Id.* at art. 25(2).
38 *Id.* at rec. 83.
39 *Id.* at art. 32.
40 A data protection supervisory authority is a person appointed by domestic legislation in each EU Member State to implement and enforce the GDPR.
41 GDPR, *supra* note 2, at art. 33.
42 *Id.* at art. 37(1)(b).

"regular and systematic monitoring" (as used in Article 37(1)(b)) and interpreted "regular" as meaning ongoing or repeated at particular intervals and found "systematic" to include "taking place as part of a general plan for data collection."[43] Some examples they gave include closed circuit television ("CCTV"),[44] but this would also likely apply to high resolution remote sensing.

A company's DPO must be involved in all issues relating to data protection within the company, and therefore must be an expert in data protection laws and practices. As someone within an organization with the responsibility to ensure compliance with the GDPR, the DPO interfaces with data subjects as well as applicable supervisory authorities within the EU.[45] While the role of the DPO is now formalized, most medium and large-sized companies will need to have such an expert to ensure compliance with the regulations, so the actual DPO requirements may not make much practical difference for such companies.

In addition to a DPO, controllers or processors that are located outside the EU, but who fall within the jurisdiction of the GDPR by virtue of their monitoring of the behavior of data subjects within the EU,[46] must designate a representative in the EU. This representative must be established in an EU Member State where data subjects who are being monitored are located.[47] Such representative will serve as the point of contact for the DPAs in each EU Member State and will be subject to any enforcement proceedings in the event the controller or processor is not compliant with the GDPR.[48] The current DPD has a more limited representative requirement that applies to controllers not established in the EU, but who make use of "equipment" in the EU to process data.[49] A November 2016 ruling by the Administrative Court in The Hague affirmed a penalty imposed by the Dutch DPA against mobile app provider Whatsapp for failure to appoint a local Dutch representative pursuant to the Dutch implementation of the DPD. Whatsapp argued that it is impossible to comply, since this would mean finding a local representative that would have no influence on the controller's activities yet would be liable for fines and penalties. Whatsapp stated it had failed to find a

43 Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, 16/EN WP 234, *adopted* December 13, 2016, at 20-21, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.

44 *Id*. at 21.

45 GDPR, *supra* note 2, at arts. 38-39.

46 *Id*. at art. 3(2)(b).

47 *Id*. at art. 27(3).

48 *Id*. at rec. 80.

49 DPD, *supra* note 17, at art. 4(1)(c) and art. 4(2).

commercial party willing to accept such risk.[50] The Hague Court rejected Whatsapp's argument, stating that there was no such exception in the Dutch implementation of the DPD. As there is similarly no impossibility exemption in the GDPR, it may be similarly difficult for non-EU companies to find local representatives to take the responsibility for the controller's activities.

Under Article 35 of the GDPR, entities involved in data processing that "is likely to result in high risk to the rights and freedoms" of individuals are required to conduct a data protection impact assessment ("DPIA") prior to such processing. While the GDPR does not provide much insight into what activities might be considered "high risk," one example provided is the "systematic monitoring of a publicly accessible area on a large scale."[51] The recitals to GDPR explain that DPIAs are essential in such monitoring situations, "especially when using optic-electronic devices . . . in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale."[52] Further to this guidance, the Article 29 Working Party explained the reasons such large-scale monitoring could be considered high risk. In such instances, "personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s)."[53] Thus, data controllers engaged in the capture of satellite images will likely be subject to the DPIA requirements of the GDPR. The current regulations provide very little guidance on what a DPIA would require, but states that it must at least contain a description of the processing operations, the purposes of the processing, the legitimate interest of the data controller, an assessment of the necessity and proportionality of the processing in relation to such purposes, an assessment of the risks to data subjects from such processing and the measures envisaged to address such risks.[54]

III.D.2 Processors

Data controllers often appoint third-party service providers to act as processors of personal data on their behalf. The GDPR allows such

50 *WhatsApp Inc.* v. *Autoriteit Persoonsgegevens*, SGR – 15/9125 (Nov. 22, 2016), at Section 10.1, available at http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2016:14088.

51 GDPR, *supra* note 2, at art. 35(3)(c).

52 *Id.* at rec. 91.

53 Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, 17/EN WP 248, *adopted* April 4, 2017, at Section III(B)(a)(3), available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

54 GDPR, *supra* note 2, at art. 35(7).

delegation, but imposes certain requirements on the processor and data subjects can hold such processor liable for their non-compliance.[55]
Article 28 sets forth the specific requirements of a data processor. A controller must engage a processor through a binding agreement that sets out the details of the processing to be undertaken by the processor. The data processor must only act in accordance with the documented instructions of a data controller; if the processor disregards the controller's instructions and makes its own decisions, the processor is then treated as a controller with respect to such activity.[56] In addition, some of the requirements discussed above with respect to data controllers also apply to data processors, including the obligations relating to data security (Article 32) and the designation of a DPO (Article 37) and an EU representative (Article 27).

IV. Considerations for Earth Observation Satellite Companies

As discussed generally above, there are a number of provisions of the GDPR that may be applicable to companies that operate earth observation satellites. The new regulations will not only have wider applicability to companies that were not previously subject to the DPD, but now impose more obligations on companies who are controlling or processing personal data. Although very little has been written about how the GDPR will apply to satellite companies, commentators and even the Article 29 Working Party have considered certain other activities that may be analogous to satellite observation, such as drones and CCTV.
Like satellites, drones have the ability to collect and record personal data in a manner that cannot easily be detected, allowing the operator to identify individual people, directly or indirectly. In the context of a study on privacy issues relating to drone usage, the European Commission identified certain risks to privacy that result from the foregoing personal data collection capabilities. These include the chilling effect of being watched, the dehumanization of those under surveillance and the loss of privacy of one's location or with whom one associates.[57] In light of these risks and the associated difficulties from a data protection perspective (e.g., consent, accountability, data security, rights of access and correction and

55 *Id*. at art. 82(1)-(2).
56 *Id*. at art. 28(10).
57 *See* Directorate General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs, *Privacy and Data Protection Implications of the Civil Use of Drones* (2015) at 20, available at www.europarl.europa.eu/RegData/etudes/IDAN/2015/519221/IPOL_IDA(2015)519221_EN.pdf [hereinafter, Privacy Implications of Drones] (citing European Commission, Communication from the Commission to the European Parliament and the Council: *A new era for aviation – Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner*, COM (2014) 207 final, August 4, 2014).

proportionality of data collection), the authors suggested certain policy recommendations,[58] some of which could be equally applicable to satellites as they are to drone activities. Among the policy suggestions, the authors proposed the development and implementation of "information and transparency protocols"[59] in which operators provide information (e.g., through a database or website) about missions and the data collected thereunder. While this may be easier in the context of drone activities, it is certainly something satellite operators should consider. Other recommendations in the policy paper, including encouraging "privacy by design and by default," conducting impact assessments and creating codes of conduct will be discussed below, and are now requirements under the GDPR.
The Article 29 Working Party also considered certain data protection issues related to the use and operation of drones. After making many of the same observations as the authors of the *Privacy Implications of Drones* study, the Article 29 Working Party noted that their drone guidelines would apply equally (with necessary adjustments) to data processing arising from the use of any aerial vehicle (including satellites).[60]
For any company or person under the jurisdiction of the United States, the operation of remote sensing satellites requires a license from the National Oceanographic and Atmospheric Agency ("NOAA").[61] Among other obligations, NOAA requires all applicants to submit a Data Protection Plan that contains a process for protecting data throughout the entire cycle of collection, processing, storage and dissemination.[62] While the Data Protection Plan requirements do not currently have any specific requirements with respect to privacy or the protection of personal data, it has been suggested that this is something NOAA could consider.[63] As noted earlier, even if it is not yet formally part of the regulatory requirements from NOAA, companies operating remote sensing systems will likely be subject to the GDPR, and so such consideration about how to maintain compliance with data protection laws will nonetheless be imperative.
One example of an implementation of privacy by default and by design that fits into the GDPR's mandate for proportionality of data collection would be a means of anonymizing personal data that is collected. If the collection of satellite images does not require images of identifiable people, remote sensing

58 Privacy Implications of Drones, *supra* note 57, at 21-25.
59 *Id.* at 25.
60 Article 29 Data Protection Working Party, *Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones*, 01673/15/EN WP231, *adopted* June 16, 2015, at 9 [hereinafter, WP29 Opinion on Drones].
61 15 C.F.R. § 960 (2006).
62 15 C.F.R. § 960.11(b)(13) (2006).
63 Janna J. Lewis & Lauren R. Caplan, Drones to Satellites: Should Commercial Aerial Data Collection Regulations Differ by Altitude?, 11 SciTech Lawyer 10, 12 (2015).

companies should consider a mechanism to automatically process images by blurring faces or other identifying information. Given the ever-increasing ability for artificial intelligence to identify individual people in digital photographs, blurring will become even more important as a means of ensuring data collected is proportional to the need for such data.[64] Google Street View currently does this for all faces and license plates and will blur images of houses and cars upon request.[65] As image resolution improves, even if the data is required for particular purposes for a certain amount of time, personal data that is no longer needed should generally be anonymized or disposed of as promptly as possible.

Article 40 of the GDPR discusses the creation of codes of conduct by industry groups representing particular industries acting as data processors or data controllers. Such codes of conduct will be drafted up by the applicable industry groups and adopted by the European Data Protection Board that will be set up once the GDPR goes into effect. While laborious to create, a code governing the proper protection of personal data for remote sensing satellite operators would be a positive industry-wide step toward helping such companies ensure they will not run afoul of the European data protection regulations. Such an industry group could also help remote sensing companies conduct any necessary DPIAs required under Article 35.

V. Remote Sensing Applications for Refugees

The GDPR recognizes that "the right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."[66] One example of this relates to the important use of high resolution satellite images is to monitor refugee migration patterns and map refugee camps in order to better provide humanitarian aid. High resolution satellite images can provide researchers and relief workers better information about the number of refugees in a camp and the locations or layout of buildings and temporary shelters. And by determining the sizes of refugee tents, it is possible to estimate the number of people such tent may

64 *See* WP29 Opinion on Drones, *supra* note 60, at 14. *See also* Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, 00720/12/EN WP193, *adopted* April 27, 2012; Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 0829/14/EN WP216, *adopted* April 10, 2014.

65 *Image Acceptance & Privacy Policies*, Google Street View, https://www.google.com/streetview/privacy/#service-use (last visited Sept. 6, 2017) (describing Google's blurring policies).

66 GDPR, *supra* note 2, at rec. 4.

hold.[67] High resolution satellite images have also been used to detect and rescue migrants in inflatable boats.[68] In situations where collecting information from the ground is dangerous, expensive and inefficient, high resolution images from space can provide a means of capturing it much more easily and safely. That said, despite all of the positive effects satellite surveillance has for assisting migrant and refugee populations, there are also dangers. The ability to track individual people could easily be used for discriminatory purposes and people could be more easily tracked and caught before they reach the safety of another country's borders.

Given the important need to track changes in refugee populations and their locations, it is likely that increased satellite time and greater scrutiny will be given to such crisis areas. As more eyes will be focused on such an already-vulnerable population, it is all the more important to consider a balance between each fundamental human right – safety and security on the one hand, and a right to privacy on the other. This is not to say that non-governmental organizations and others who are involved in humanitarian aid may disregard the GDPR as it would apply to such monitoring of European citizens. However, in the case of a developing humanitarian crisis situation, the collection of certain sensitive personal data, the processing of which is otherwise highly restricted (e.g., data revealing racial/ethnic origin or biometric data for the purpose of uniquely identifying a natural person) may be allowed. In fact, the concern over protection of such personal data with respect to refugees is evident due to the fact that the UN High Commissioner for Refugees ("UNHCR") has issued a Policy on the Protection of Personal Data of Persons of Concern to UNHCR.[69]

The GDPR allows processing of such data "where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person."[70] Some examples that the GDPR gives for such processing that serve the public interest and the vital interests of the data subject include humanitarian purposes (e.g., in the event of man-made or natural disasters).[71] Furthermore, there are carve-outs that allow for the transfer of personal data without explicit consent, in the event that the transfer is to an international

67 *See*, *e.g.*, *Satellite Intelligence: A Solution to the Refugee Crisis?*, EARTH-I LTD., http://earthi.space/blog/satellite-solution-refugee-crisis/ (last visited Sept. 6, 2017).

68 *See*, *e.g.*, *Frontex Eurosur Services Help Rescue 370 People Off Libyan Coast*, European Border and Coast Guard Agency (FRONTEX), http://frontex.europa.eu/news/frontex-eurosur-services-help-rescue-370-people-off-libyan-coast-MxXy7S (last visited Sept. 10, 2017) (although Frontex is an EU agency that uses EU satellites to monitor European borders, including with respect to migrants' movement, private satellite data could similarly be used by governments, NGOs or private companies).

69 UN High Commissioner for Refugees (UNHCR), *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* (May 2015).

70 GDPR, *supra* note 2, at rec. 46; *see also*, *id.* at art. 9(2)(g).

71 *Id.* at rec. 46.

humanitarian organization and is to be used for "accomplishing a task incumbent under the Geneva Conventions or to complying with international humanitarian law applicable in armed conflicts."[72]
Organizations involved in providing humanitarian aid wishing to use high resolution satellite images and those companies providing the data, should be aware of the data protection obligations in the GDPR. This includes taking proactive steps prior to any processing to ensure compliance, including carrying out a DPIA that clarifies the risks and considers mitigation measures or other safeguards that could be put in place.[73]

VI. Conclusions

The satellite imaging business is a growing industry and the resolutions that these satellites can achieve continue to improve. Even though the U.S. currently puts a at 0.25 m restriction on the minimum resolution of commercial images, lobbying from the industry has steadily decreased this limit. Better raw data, together with a lower cost of launching satellites and the dramatic improvement in computing power, make the processing and data extraction from such images increasingly easier. Facial and other image recognition software already allows users to extract specific details from vast troves of images, but this technology is rapidly improving, especially with the rise of artificial intelligence and neural networks. While access to high quality satellite data has many commercial, law enforcement and military applications, the ease with which such information may be accessed and processed raises concerns about privacy and the need to ensure protection of personal data.
Even though the GDPR does not specifically address the risks associated with the collection and processing of high resolution satellite images, it is a regulation that is intended to be broad enough to capture many new forms of technology that may affect privacy. For this reason, it is incumbent upon commercial satellite operators to be aware of the scope and jurisdiction of the regulation, as it is very likely to be applicable. Given the increased territorial reach of the GDPR and the obligations it imposes, it is important for commercial satellite operators, as well as those companies who use and process images from such satellites, to be aware of the regulation and to ensure their compliance before the GDPR goes into effect on May 25, 2018.

72 *Id.* at rec. 112.
73 International Committee of the Red Cross, Handbook on Data Protection in Humanitarian Action, 107 (Christopher Kuner & Massimo Marelli, eds., 2017).