# The Application of Data Protection Laws in (Outer) Space

Martin M. Zoltick

Rothwell Figg

Jenny L. Colgate

## I Introduction

We live in a rapidly changing world, and nothing is evolving faster than the information and communication technologies that have become a part of almost every aspect of our daily lives. While some of us can remember a time without the Internet, smartphones, search engines, and digital assistants – those days are long gone. We live in a digitalised society, and we expect to have the information we want and the ability to control our lives literally at our fingertips – simply by querying Google, by tapping a button on an app, or by asking Siri or Alexa.

Our communications infrastructure and the hardware devices and computer software that comprise it have been transformed into network-connected devices, systems, and services – often referred to as the "Internet of Things" or "IoT" – that are "smart". "The widespread incorporation of 'smart' devices into everyday objects is changing how people and machines interact with each other and the world around them …."[i] Devices, systems, and technologies, such as smart thermostats, are installed in our homes, and predict our living patterns and temperature preferences. Our smartphones and digital assistants anticipate the information we are likely to want, when we want it; for example, telling us the news we care about before we even know to ask. And instead of our GPS responding to our inquiry for directions, it anticipates where we will likely want to go at a particular time of day based on our past travel, and sends us alerts as to where our car is parked, and how long it will take to get to work based on current traffic.

While the benefits of the aforementioned devices and services to society, to our economy, and to us as individuals are undeniable, "their deployment has also introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Cyber actors have already used IoT devices for distributed denial-of-service (DDoS) attacks, and we assess they will continue. In the future, state and non-state actors will likely use IoT devices to support intelligence operations or domestic security or to access or attack targeted computer networks."[ii] The most significant challenges in addressing such unauthorised access and attacks, and in enforcing data protection laws, rules, and regulations, are the difficulties of dealing with cross-border issues (*e.g.*, cross-border flows of data) and accompanying choice-of-law issues.

The legal system is trying to keep up, but it is doing so based on the constructs of nation states and regional laws; a two-dimensional system with artificial boundaries regulating a three-dimensional boundary-free environment. In today's world, we regularly travel – across state lines and country lines, across continents and oceans. And as we travel, we generate data about ourselves. We make purchases with credit cards; join WiFi hotspots; use our apps; we tweet; post; talk to Siri and Alexa; wear a fitness tracker or smart watch; check in at the gym; use GPS; use "smart" appliances; shop online; and the list goes on. Trying to determine which data protection laws, rules, and regulations apply to us, and to our data, as we move about the world, is confusing and complex. And even if we as individuals stay put, the data about us travels the world – and beyond. Our home-town gym may contract with a network of other gyms that span the globe, sharing our information across multiple continents ***and into outer space*** by transmitting the data via satellite. The benefit to us is that we can go anywhere, and it's "just like home". We can go anywhere and stay "connected". We may not physically be at home, but we can control our "smart devices" remotely, or just let them take control. The drawback to us is that our personal data is everywhere, and trying to track it and control it – let alone stay on top of our rights, via the patchwork of regulations that apply to our personal data based on where it was collected, transmitted and/or processed, who is controlling the collection, transmission and/or processing, and who is doing the collecting, transmitting, and/or processing – is a formidable task even for a seasoned data protection expert. Equally as challenging, from the standpoint of the data controller or processor, is determining in such an ecosystem, what is required for compliance, the metes and bounds of the privacy programme to implement, the incident response programme to employ, and what type of impact assessment is required.

The future will only get more complex unless the legal system adapts and changes. There are simply too many different laws governing – in many cases – the same personal data. According to the United Nations Conference on Trade and Development, as of April 2, 2019 there were 107 countries with (different) legislation in place to secure the protection of data and privacy.[iii] In addition, there were at least 14 countries that were in the process of drafting legislation, and there were a number of regional groups that were aimed at unifying the laws of countries in certain regions.[iv] However, unlike the GDPR – which displaced the domestic data protection laws of countries in the EU – other regional laws do not displace countries' domestic laws. For example, in Asia, the Asia-Pacific Economic Cooperation (APEC) Privacy Framework developed uniform data protection laws – called the APEC Cross-Border Privacy Rules (CBPR) system – but unlike the GDPR, the CBPR system does not displace or change a country's domestic laws or regulations.[v]

Adding further to the complexity of the legal landscape, there are also some laws that are industry-specific. This is especially common in the United States. For example, the Communications Act of 1934 imposes data privacy and security requirements on "cable operators" and "satellite carriers."[vi] And while there are some entities that are governed by a patchwork of data protection laws, others seemingly

fall through the cracks entirely and are governed by none. For example, currently non-profits are exempt from the California Consumer Privacy Act,[vii] and international intergovernmental organisations like the European Space Agency (ESA) are exempt from the GDPR.[viii]

All of this is to say that now may be the perfect time for countries around the globe to discuss a set of global data protection standards. People and companies are only getting more transitory. It is less clear than ever before where a "company" is actually located because often in today's world a company is a network of individuals working collaboratively from remote locations. And the current landscape of trying to determine where and by whom personal information is collected, transmitted and processed will only get murkier in the future, as the world continues to "grow up" into outer space. Of course, realising the unlikelihood of a set of global data protection standards, the authors propose that at the very least a new treaty, or new international rules and/or regulations, should be considered addressing data protection laws in outer space.

Space tourism is a growing industry, and while no tourist has been to space since 2009, some are saying that 2019 is the year this is going to change, as a number of private companies, such as VirginGalactic, BlueOrigin, SpaceX, and Boeing, have been working diligently to fulfil promises of taking humans to space.[ix] Drones are becoming a part of everyday life. They are used for surveillance (everything from catching lawbreakers, to tracking down pipeline leaks, to monitoring the impacts of climate change on wildlife); they take pictures from the air (such as action photos of extreme sports and property pictures for realtors); they are used to help film Hollywood movies; there are military applications; and some commercial enterprises are even exploring – or implementing – the use of drones to deliver goods to people.[x] In April 2019, Google's drone delivery service was approved for public use in Australia.[xi] It is only a matter of time before drones are used in outer space. Drones are already operating in "near space" – the area between where airplanes safely fly within the "domestic airspace" above the countries below, and where outer space begins.[xii]

Also, we have an emerging space infrastructure and the deployment of space and terrestrial components, products, and services that are becoming an essential part of the ecosystem of interconnected devices and services. Companies and organisations are already working to realise the promise of satellite-powered networks that would bring the IoT to everywhere in the world. For example, the "Internet of Things Everywhere on Earth" (IOTEE) Project is a project that has been funded by the European Union to provide IoT Low-Power Wide-Area (LPWA) services from space. As another example, Amazon Web Services (AWS) recently struck a deal with satellite provider Iridium to develop a satellite-based network called CloudConnect, designed specifically for IoT applications, to "bring internet connectivity to the whole planet". And in October 2018, SemTech and Alibaba Cloud agreed to develop an IoT network in China using small satellites in low Earth orbit.[xiii]

Global Positioning System (GPS) technology is also an area of growing technological development that involves outer space and data protection issues. GPS involves multiple satellites in the Earth's atmosphere transmitting signals to devices that can determine the current location on the ground. The satellites began being launched in 1978 and have since grown to a network of 24 global satellites, which give full coverage for GPS navigation everywhere. GPS was originally used by aviation pilots for navigation; then it expanded into expensive road vehicles, followed by inexpensive portable units for vehicles; and today our communication and media devices routinely make use of GPS technology, tracking where you and your personal property are located.[xiv]

In this chapter, we explore a variety of legal issues that would likely come into play when dealing with the processing of personal data in outer space considering the existing patchwork of regulations and treaties. We also propose that a new outer space treaty should be negotiated, or new international rules and regulations adopted, providing data protection minimum standards and making clear which law(s) govern the collection, use, disclosure, retention, and disposal of personal data or personally identifiable information (PII) in outer space. The space infrastructure and deployment of space and terrestrial components, products, and services is rapidly evolving and, we submit, now is the time to seriously consider making regulatory changes so that our data protection laws are better suited to deal with the future ahead of us.

## II A Hypothetical to Explore the Current Regime of Applicable Law

To explain the current situation with the law, we will use a hypothetical scenario – imagine that due to technological advances, a space data-centre start-up has built a space-based data-centre platform that will operate in Low Earth Orbit (LEO) at 58 miles above sea level (8 miles higher than NASA considers "outer space" to begin). (Note: Currently, low earth orbit satellites operate in the first 100-1,200 miles above Earth.[xv,xvi] However, "[i]n theory, it is only the horizontal speed which decides whether a satellite goes into orbit", such that the lower the altitude above earth, the higher the required orbital velocity.[xvii]) The company claims that the benefit of its data-centre over other space data-centres is that due to its proximity to Earth, communication is faster and its services are less expensive.[xviii] Like other space data-centres, it claims its system of LEO satellites (LEOS) is an alternative to Internet-based data storage and services, which are notoriously insecure. The company seeks your legal advice to ensure that, because it operates in outer space (right at the Karman line), it is not subject to any data protection regulations.

### a. Are the LEOS in Airspace or Outer Space?

A threshold issue for determining what regulations would apply in outer space is resolving the issue of *what is outer space*. Where does airspace end and outer space begin?

There is currently no internationally agreed upon answer to this question. The most accepted "norm" to define the point at which the airspace above a country ends and outer space begins is a boundary called the Karman line. For decades, the *Fédération Aéronautique Internationale* (FAI) has set the Karman line at 100 kilometres or 62 miles high.[xix] But again, this is not a universal standard, and even the US Air Force and NASA do not abide by this limit; instead, treating the line as 50 miles.[xx]

In view of the foregoing, it would be difficult to advise the client whether outer space or airspace laws are applicable.

### b. Airspace Law

Unfortunately, application of the law only gets more complex from there.

A basic principle of international air law, which was affirmed in Article 1 of the Paris Convention on the Regulation of Aerial Navigation (1919) and subsequently by various other multinational treaties, is that every state has complete and exclusive sovereignty over the airspace above its territory, including its territorial sea.[xxi] Thus, airspace is generally considered an appurtenance of the

subjacent territory and shares the latter's legal status. Accordingly, international law that applies to the High Seas (i.e., non-territorial seas) also applies to airspace above the High Seas, vertically up to the point when airspace ends and outer space begins, at which point the Outer Space Treaty applies.[xxii]

The aforementioned would suggest that as the LEOS orbit the Earth, so long as they are lower than "outer space" (an undefined boundary), they would be subject to the data protection laws of any country above which they pass over, as well as whatever applicable laws apply to personal data on the High Seas, to the extent they are passing over non-territorial waters. Obviously, ensuring compliance with so many countries' data protection laws would be unwieldy and impractical. We note that these issues would likely not arise for a geostationary satellite, which stays in one location relative to a specific spot on earth.

There are also a number of airspace treaties that could potentially apply to further address the choice-of-law questions regarding which countries' data protection laws would apply, particularly in the event of a data breach. For example, historically, when a crime has been committed during an international flight, there have been difficulties pinpointing when and where it occurred and hence in determining which nation's laws may have been violated (or in the case of violations that occur in airspace over the High Seas, whether there is any applicable law).[xxiii] The same would be true with respect to a data breach of a LEOS. The 1963 Tokyo Convention on Offenses and Certain Other Acts Committed on Board Aircraft provided that in addition to the law of the nation where the violation occurred applying, nations may also extend their criminal law and jurisdiction to aircraft of their registry when they are outside national territory.[xxiv] Notwithstanding, it is not clear if this convention would even apply to LEOS, as it seems to apply only to manned aircraft. Further, this convention is limited to "offenses against penal law", and thus would not apply to data protection regulations that impose only civil remedies.

There are also laws and treaties addressing civil offences that occur in airspace, but there is no general principle that the law of the nation of registry of the aircraft applies to all civil offences that occur on board (to parallel the aforementioned Tokyo Convention on criminal acts). Instead, there is a patchwork of international agreements that affect the exercise of civil jurisdiction by nations, and their application to data breaches on unmanned LEOS (as opposed to traditional civil offences on manned aircraft) is as imperfect as the application of the Tokyo Convention discussed above. For example, the 1929 Warsaw Convention for the Unification of Certain Rules Relating to International Carriage by Air applies "to all international carriage of persons, luggage or goods performed by aircraft for reward", and would presumably not apply to the processing of data by a LEOS.[xxv]

Additionally, there is a further choice-of-law question to the extent the LEOS pass over the High Seas. Article 92(1) of the United Nations Convention on the Law of the Seas (UNCLOS) provides that ships shall sail under the flag of one state only and, "save in exceptional cases expressly provided for in international treaties or in this Convention, shall be subject to its exclusive jurisdiction on the high seas".[xxvi] One of the "exceptional cases" identified in Articles 101–107 of the convention concerns piracy. Article 105 provides that "[o]n the high seas, or in any other place outside the jurisdiction of any state, every state may seize a pirate ship or aircraft, or a ship or aircraft taken by piracy and under the control of pirates, and arrest the persons and seize the property on board". Again, the issue here is that the language of the treaty does not clearly apply to data piracy, where there may be no "pirate ship or aircraft", and indeed the "pirates" may be located far away from the property (personal data) being seized. The definition of "piracy" in Article 101 similarly is focused on "crews" and "passengers" of ships and aircraft.[xxvii]

In sum, trying to advise a client regarding the data protection legal framework that would apply to a network of LEOS processing personal data – even assuming it is a given that they are in airspace and not outer space – would be next to impossible, just from a choice-of-law standpoint. There are multitudinous treaties and conventions that could potentially apply, but the applications are stretched and imperfect.

### c. Outer Space Law

The application of outer space law to data protection issues is no different.

Outer Space law began in 1959, shortly after the Soviet launch of the first artificial satellite into space (Sputnik 1), with the creation of the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS).[xxviii] COPUOS was formed during the "space race" period between the United States and the Soviet Union, with the mission of ensuring that outer space is used for peaceful purposes.[xxix] In 1966, the UN drafted Resolution 2222 (XX1), the "Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies", also known as the "Outer Space Treaty". The Outer Space Treaty was founded on similar principles to those of COPUOS, including a recognition of "the common interest in all mankind in the progress of the exploration and use of outer space for peaceful purposes" and "believing that the exploration and use of outer space should be carried on for the benefit of all peoples irrespective of the degree of their economic or scientific development".[xxx]

The Outer Space Treaty and other similar outer space treaties (e.g., the Space Liability Convention and the Registration Convention) – like the treaties and conventions on airspace and the High Seas – do not cleanly apply to the issues of data protection. They were drafted before the time of data, and do not even begin to contemplate the commercial use of outer space for, *inter alia*, data processing. Notwithstanding, like the airspace and High Seas treaties, there are some provisions of the outer space treaties that address liability generally, which could arguably be stretched to cover data protection and breaches in outer space.

For example, Article VII of the Outer Space Treaty provides that each State Party to the Treaty that launches or procures the launching of an object into outer space, and each State Party from whose territory or facility an object is launched, is internationally liable for damages to another State Party to the Treaty or to its natural or juridical persons by such object or its component parts on the Earth, in air or in outer space. Presumably, this could mean that a country could be liable to another country, to the extent that an object launched from the first country resulted in a data breach of "juridical persons" of the second country, but only if the data breach would occur by launching an object into space (an unlikely scenario).

Another example of an issue with applying the Outer Space Treaty to data protection is that it seemingly provides for the ability to game the system. Article VIII provides that "[a] State Party to the Treaty on whose registry an object is launched into outer space … shall retain jurisdiction and control over such object, and over any personnel thereof, while in outer space". In other words, if one's space-processed data is hacked by another object that is launched into space, then the data protection laws of the country from which the object was launched into outer space would retain jurisdiction over any legal claims relating to the damage. The issue here is that bad actors could potentially avoid legal consequences by simply "launching" (or acting/breaching) from a country where there are no data protection laws. For example, of the 135 countries that are parties to the Outer Space Treaty, 30 countries appear to have no

national data protection laws, and an additional 13 only have draft data protection legislation.[xxxi]

In view of the foregoing, it would be difficult to advise a client of the possible data protection laws that would apply to an outer space data-centre. One could comfortably say that the other space treaties are only concerned with liability. Thus, unless a breach occurs, it is probably fair to say that there are no data protection regulations that extend to outer space. In the event of a data breach, it is possible that the outer space treaties would be stretched to extend domestic data protection regulations to cover the breach, such as by applying the law of the nation where the breaching party resided (even if they did not "launch") or the law of the nation whose object/data is hacked.

### d. Shortcomings of Existing Data Protection Regulations

The aforementioned discussions of international law regarding airspace, the High Seas, and outer space were all concerned with choice-of-law issues, i.e., determining if there is a regulatory framework in place that establishes what law(s) apply. As discussed above, the answer is that for a lot of new technologies – satellites, drones, aircraft, commercial space objects, IOT devices, and so forth – the international choice-of-law rules do not clearly apply. But even if they did clearly apply, there is still another issue, and that is that the domestic data protection laws do not clearly apply outside of Earth.

By our calculation, there are at least 118 countries in the world today with data protection laws in place, and another 19 in the drafting process.[xxxii] Because it is not feasible for us to discuss each of these laws here, we will be focusing on two – the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) (which goes into effect on January 1, 2020). For the reasons we explain below, we believe both regulations apply to personally identifiable information processed in outer space, but there is a loophole in the GDPR that could allow companies processing PII data in outer space to shirk their otherwise applicable GDPR obligations.

#### i. GDPR

The territorial scope of the GDPR's application is broad. It applies to: (1) the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not; (2) the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where processing activities are related to (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or (ii) the monitoring of their behaviour as far as their behavior takes place within the Union; and (3) the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.[xxxiii]

Given the breadth of the aforementioned terms, it is easy to imagine possible scenarios where the GDPR could apply in outer space – for example, a controller or processor that is located in the EU and processes personal data via a satellite located in outer space; satellite Internet, GPS, and media providers that offer their services to customers in the EU; and a space data-centre that is based in the EU or processes data about individuals located in the EU. In all of these situations, the GDPR seemingly applies.

The one area where the GDPR seemingly missteps is with respect to transfers of data to outer space. Chapter 5 governs "[t]ransfers of personal data to third countries or international organizations". However, Chapter 5 (and the rest of the GDPR) is silent with respect to transfers of data outside of the Earth.

Article 44, the first article of Chapter 5, provides:

> Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.[xxxiv]

Thus, even though the territorial limitations of Article 4 of the GDPR are broad enough to cover data processed in outer space, the regulations regarding transfers of data – from Chapter 5 – are limited to transfers on Earth. This means that to the extent an individual engages with a business that is ordinarily subject to GDPR protections, there is a potential loophole that the business could rely on – to the extent it processes data in outer space – to shirk its otherwise applicable GDPR obligations.

#### ii. CCPA

Our reading of the CCPA is that there is no similar loophole. Section 1798.150 of the CCPA provides a broad obligation on the part of businesses to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information", and provides that, to the extent a third party gains unauthorised access and exfiltration, theft, or disclosure results as a consequence of the business's violation of its duty to implement and maintain such security procedures and practices, then damages, injunctive or declaratory relief, or any other relief that the court deems proper could result.[xxxv] Thus, because section 1798.150 applies regardless of where data is being processed – and further because there are no provisions that are limited to transfers of data on Earth – the "outer space loophole" of the GDPR has been avoided.

In sum, this short analysis of the GDPR and the CCPA is just to highlight the fact that the issues with the application of existing regulations to the future of the processing of PII in air and outer-space is not just an international law problem. It is also something that each nation should consider with respect to its own regulations, to ensure that there are no unintended loopholes in its data protection laws that could apply when personal data is processed in outer space.

## III Future International Treaty, Rules, or Regulations

Given the above analysis, it is clear to the authors that new international laws, rules, and/or regulations are needed to more clearly establish which data protection laws apply when personal data is processed in air and space. Current international air law and High Seas law addresses criminal and civil law through a patchwork of rules that do not clearly apply to unmanned aircraft or devices processing personal data, and the outer space treaties are concerned only with liability, and arguably do not extend to govern compliance or to establish liability for failures to comply or as a result of data breaches (without corresponding physical altercations). As such, a legal framework – such as in the form of a data protection treaty – should be negotiated, or a set of rules and/or regulatory standards – perhaps under the authority of the International Telecommunication Union ("ITU")[xxxvi] – should be drafted applicable to the protection of personal data in airspace above nations, above the High Seas, and in outer space. Such laws, rules and/or regulations could provide much needed clarity to choice-of-law issues and, thus, requirements for compliance, required actions upon a data breach, enforcement and remedies.

In determining the applicable choice-of-law provisions, care should be given to ensure that: (1) objects processing data in airspace/outer space would not be subject to the laws of every nation over which they pass; and (2) the applicable law should not be determined based on a data hacker's activities (such that hackers could position themselves in a jurisdiction without data protection laws, in order to avoid legal consequences for their actions). Logical choices for which law should apply would be: (1) the law of the country from where the object processing the personal data being hacked is launched or takes off applies; (2) the law of the country in which the entity controlling or processing the data resides applies; or (3) the law of the country where the data subjects whose data is being processed reside applies.

Additionally, a treaty (or other rules and/or regulations) should set forth minimum standards for data protection that apply once the data being processed pass a certain threshold (i.e., so as to exclude personal drones and similar devices), to ensure a minimum international standard for data protection in air and space. For example, similar to the treaties on air and outer space, there should be registries to record objects that are processing data in air and space (separate and apart from the registries of objects launched into outer space generally). Data protection inventory assessments (DPIAs), similar to those required by the GDPR, should also be compulsory in order for persons and entities to process data in outer space (and high airspace, as of a certain altitude). Additionally, a set of minimum requirements governing participating persons' and entities' processing of personal data should be specified and certification (or self-certification) should be stipulated in order for entities to process personal data in high air and outer space, similar to the US-EU "Privacy Shield" and white lists/black lists under the GDPR. The adoption of the aforementioned framework would provide for better data protection through design (including a "baseline" set of data protection requirements) and better transparency regarding the types and amounts of data that are being processed in high air and outer space.

## Conclusion

The age of personal data is here, and technological advances are shrinking the world we live in – not just two-dimensionally, but up into airspace and outer space, as well. Unfortunately, existing legal frameworks do not sufficiently address which laws apply to personal data in airspace and outer space, and as such, a new international treaty or set of rules and/or regulatory standards is needed to fill this gap, lest there be legal uncertainty which could impede the adoption of innovative technologies. Additionally, nation states should be careful to consider air and space issues when drafting their data protection laws, to ensure that there are no unforeseen loopholes where personal data is processed in outer space.

i. Daniel R. Coates, Director of National Intelligence (appearing before the Senate Select Committee on Intelligence to provide the U.S. intelligence community report on Worldwide Threat Assessment (May 11, 2017)).

ii. Daniel R. Coates, US Director of National Intelligence (appearing before the Senate Select Committee on Intelligence to provide the U.S. intelligence community report on Worldwide Threat Assessment (May 11, 2017)).

iii. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (accessed April 4, 2019).

iv. *Consumers International*, "The State of Data Protection Rules Around the World: A Briefing for Consumer Organizations", available at http://www.consumersinternational.org/media/155133/gdpr-briefing.pdf.

v. *Id*.

vi. "Satellite carriers" are defined as any "entity that uses the facilities of a satellite or satellite service . . . to establish and operate a channel of communications for point-to-multipoint distribution of television station signals . . . ." 47 U.S.C. § 338(k)(7); 17 U.S.C. § 119(d)(6).

vii. *See* California Consumer Privacy Act of 2018 (applies to "businesses", and "business" is defined as a legal entity organised or operated for the profit or financial benefit of its owners which meets certain criteria).

viii. Harebottle, Adrienne, "GDPR is Here But, What Does It Really Mean for Satellite?" available at https://www.satellitetoday.com/business/2018/05/30/gdpr-is-here-but-what-does-it-really-mean-for-satellite/ (accessed May 2, 2019).

ix. O'Callaghan, Jonathan, "2019 is the year that space tourism finally becomes a reality. No, really." (*WIRED* Jan. 24, 2019), available at https://www.wired.co.uk/article/spacex-blue-origin-space-tourism.

x. Spring, Tom, "IN PICTURES: 15 current and future uses for drones" (*ComputerWorld*), https://www.computerworld.com.au/slideshow/521205/pictures-15-current-future-uses-drones (accessed April 12, 2019).

xi. Perry, Alex, "Google's drone delivery service just got approved for public use in Australia" (*Mashable* Apr. 10, 2019), http://mashable.com/article/google-wing-alphabet-australia-canberra/#vvKAdULv8aqC (accessed April 12, 2019).

xii. *See* Chow, Eugene K., "America is No Match for China's New Space Drones" (*The National Interest* Nov. 4, 2017), https://nationalinterest.org/blog/the-buzz/america-no-match-chinas-new-space-drones-23039 (accessed April 12, 2019).

xiii. Paul, Frederic, "The Internet of Things has largely been an earthbound phenomenon. That could be about to change." (*NetworkWorld* Oct. 23, 2018), available at https://www.networkworld.com/article/3315736/is-the-iot-in-space-about-to-take-off.html.

xiv. Adamson, Benjamin, "Gps Navigation: Then, Now, and The Future" (*Street Directory*), https://www.streetdirectory.com/travel_guide/117579/gps_vehicle_tracking/gps_navigation_then_now?and_the_future.html (accessed April 12, 2019).

xv. "How High is Space" (chart of altitudes and objects in space), http://www.spacetoday.org/SolSys/Earth/AltitudesChart.html (accessed April 12, 2019).

xvi. Nelson, Patrick, "Data should be stored in space, firm says" (*NetworkWorld* June 9, 2019), https://www.networkworld.com/article/3200242/data-should-be-stored-in-space-firm-says.html (accessed April 12, 2019).

xvii. Subramanian, Krishna Kumar, "What is the lowest possible stable Earth orbit?" (Feb. 23, 2019), https://www.quora.com/What-is-the-lowest-possible-stable-Earth-orbit (accessed April 12, 2019).

xviii. *See* Hussaini, Umair, "Low earth orbit, medium and high earth orbits – Types of orbits" (*TechnoByte* Nov. 5, 2018), https://www.technobyte.org/satellite-communication/low-medium-high-earth-orbits-types-of-orbits/ (accessed April 12, 2019).

xix. Grush, Loren, "Why Defining the Boundary of Space may be Crucial for the Future of Spaceflight" (*The Verge* Dec. 13, 2018), https://www.theverge.com/2018/12/13/18130973/space-karman-line-definition-boundary-atmosphere-astronauts (accessed April 3, 2019).

xx. *Id*.

xxi. Cheng, Bin, "Air Law" (*Encyclopedia Britannica* Apr. 4, 2019), https://www.britannica.com/topic/air-law (accessed April 12, 2019).

xxii. *See id*.

xxiii. *Id*.

xxiv. *Id*. *See also* Convention on offences and certain other acts committed on board aircraft, https://treaties.un.org/doc/db/terrorism/conv1-english.pdf (accessed April 12, 2019).

xxv. United Nations Conference on Trade and Development, "Carriage of Goods by Air: A Guide to the International Legal Framework" (June 27, 2006), https://unctad.org/en/Docs/sdtetlb20061_en.pdf (accessed April 12, 2019).

xxvi. United Nations Convention on the Law of the Seas (UNCLOS) (Dec. 10, 1982), https://www.jus.uio.no/english/services/library/treaties/08/8-01/unclos.xml#treaty-header1-7 (accessed April 12, 2019).

xxvii. *Id*.

xxviii. United Nations Office for Outer Space Affairs, "Members of the Committee on the Peaceful Uses of Outer Space", http://www.unoosa.org/oosa/en/members/index.html (accessed April 2, 2019).

xxix. United Nations Office for Outer Space Affairs, "Members of the Committee on the Peaceful Uses of Outer Space", http://www.unoosa.org/oosa/en/members/index.html (accessed April 2, 2019).

xxx. UN Resolution 2222 (XXI): "Treaty on Principles Governing the Activities of States in the Exploration and Use of Other Space, including the Moon and Other Celestial Bodies" (Dec. 19, 1966).

xxxi. *See* Appendix (online): Mapping of Countries with Data Protection Laws and Signatories to Space Treaty, https://iclg.com/theme/assets/img/iclg/DP19_Space-Treaty-Signatories.pdf.

xxxii. *See* Appendix (online): Mapping of Countries with Data Protection Laws and Signatories to Space Treaty, https://iclg.com/theme/assets/img/iclg/DP19_Space-Treaty-Signatories.pdf.

xxxiii. GDPR, Article 3.

xxxiv. GDPR, Article 44.

xxxv. CCPA, section 1798.150.

xxxvi. *See* https://www.itu.int/en (accessed April 28, 2019). (ITU is an agency of the United Nations that is responsible for issues concerning information and communications technologies, including: setting standards for technologies (such as 3G and 4G mobile standards, HDTV and other television standards) and coordinated universal time (UTC); coordinating the shared use of the radio spectrum; and creating and maintaining an orbit/spectrum international regulatory framework that, *inter alia*, seeks to ensure interference-free operation of radiocommunications.)

**Martin M. Zoltick**
Rothwell Figg
607 14th Street NW
Suite 800
Washington, DC 20005
USA

*Tel:* +1 202 783 6040
*Email:* mzoltick@rfem.com
*URL:* www.rfem.com

Martin M. Zoltick has been practising in the field of technology law, focusing on intellectual property matters, transactions, data protection, and privacy, for more than 25 years. A Certified Information Privacy Professional in the United States (CIPP/US), Mr. Zoltick handles matters related to cybersecurity, privacy, and data protection, including working closely with clients to ensure compliance with the evolving legal and regulatory landscape, to establish company best practices, policies, and procedures, and in carrying out privacy-related impact assessments and incident response plans. He has a degree in computer science, worked as a software engineer, and regularly represents entrepreneurs, investors, emerging businesses, middle market, and mature companies in technology and IP-related matters, including securing protection for valuable intellectual property and data, handling transactional matters and due diligence reviews, and serving as counsel in enforcement and defence proceedings.

**Jenny L. Colgate**
Rothwell Figg
607 14th Street NW
Suite 800
Washington, DC 20005
USA

*Tel:* +1 202 783 6040
*Email:* jcolgate@rfem.com
*URL:* www.rfem.com

Jenny L. Colgate is an experienced intellectual property lawyer. She is a Certified Information Privacy Professional in the United States (CIPP/US) and has experience counselling clients on matters related to privacy, data protection, and cybersecurity, as well as litigating cases concerning data misappropriation and related IP issues. Ms. Colgate was named a Washington, DC Super Lawyer "Rising Star" for IP litigation seven years in a row from 2013 to 2019.

ROTHWELL FIGG
IP Professionals

Attorneys in Rothwell Figg's cybersecurity, privacy, and data protection practice – all of whom are Certified Information Privacy Professionals in the United States (CIPP/US) – advise clients on the broad range of issues that businesses face daily in order to secure data, guard valuable intellectual property, and comply with the laws, rules, and regulations regarding privacy. We work closely with clients to recognise, respond to, and minimise the serious risks associated with the collection, use, retention, disclosure, and disposal of personal information, susceptible IP, and data; and we assist with the design and implementation of cybersecurity and data protection best practices, compliance programmes, and incident response plans to help organisations comply with the evolving data privacy requirements. In the unfortunate circumstance when a company does face a breach, we are well-situated to assist during and in the aftermath of the incident, including taking immediate corrective measures, negotiating with the relevant regulatory authorities, defending against lawsuits arising from breaches, and advising on improvements to the security and privacy programmes for the future. We also have experience successfully representing clients in privacy-related investigations initiated by the Federal Trade Commission (FTC).