# Privacy in the age of remote sensing during natural disasters in Australia and Indonesia

Lawal, Temitope; Jackson, Melanie; Georgiades, E.

*Published in:*
Digital Law Journal

*DOI:*
10.38044/2686-9136-2023-4-2-15-39

https://doi.org/10.38044/2686-9136-2023-4-2-15-39



ARTICLES

# PRIVACY IN THE AGE OF REMOTE SENSING DURING NATURAL DISASTERS IN AUSTRALIA AND INDONESIA

**Temitope Lawal*, Melanie Jackson, Eugenia Georgiades**

Bond University
14, University Drive, Robina, Queensland, Australia, 4226

## Abstract

Satellites are increasingly used for remote sensing, aiding in disaster management, however they also raise privacy concerns. Despite the existence of international instruments such as the *Outer Space Treaty, Principles Relating to Remote Sensing of the Earth from Outer Space* and *International Charter Space and Major Disasters*, there are no specific rules addressing satellite misuse leading to privacy breaches during natural disasters. This article examines the existing legal frameworks for satellite regulation and privacy in Australia and Indonesia, two disaster-prone countries, with the aim of determining their adequacy for addressing privacy concerns arising from satellite use during natural disasters. By conducting a comparative analysis of both legal frameworks vis-à-vis relevant international law, this article highlights the gaps that affect their applicability and effectiveness. It finds that international rules on the use of satellites for remote sensing activities generally lack binding force, and do not address the issue of privacy breaches resulting from satellite misuse. Both countries also lack specific legal frameworks addressing privacy breaches caused by satellite misuse during disasters. It recommends that in the absence of unequivocal and specific provisions under international law, both countries could review and rely on their national legal frameworks to address potential privacy issues due to advancing remote sensing capabilities. The provision of Article VI of the *Outer Space Treaty* requires states to authorise and ensure continued supervision of activities of non-governmental entities in outer space. This provision could be relied on to impose, through the instrumentality of domestic laws, restrictions, or conditions on space activities, including privacy provisions. Existing space legislation requiring liability insurance could also be extended to include privacy provisions.

## Keywords

data privacy, legal frameworks, natural disasters, remote sensing, satellite misuse

| | |
|---|---|
| **Conflict of interest** | The authors declare no conflict of interest. |
| **Financial disclosure** | The study was funded by the APNIC Foundation, Grant ID: F-202206-01436 — Bond University Internet Law Research Clinic: Enhancing the Efficacy of Internet Connectivity Legal Frameworks in the Asia-Pacific Region. |
| **For citation** | Lawal, T., Jackson, M, & Georgiades, E. (2023). Privacy in the age of remote sensing during natural disasters in Australia and Indonesia. *Digital Law Journal*, 4(2), 15–39. https://doi.org/10.38044/2686-9136-2023-4-2-15-39 |

* Corresponding author

Submitted: 9 June 2023, accepted: 27 June 2023, published: 31 July 2023

СТАТЬИ

# КОНФИДЕНЦИАЛЬНОСТЬ В ЭПОХУ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ СТИХИЙНЫХ БЕДСТВИЙ В АВСТРАЛИИ И ИНДОНЕЗИИ

**Т. Лаваль*, М. Джексон, Е. Георгиадес**

Университет Бонд
4226, Австралия, Квинсленд, Робина, Юниверсити Драйв, 14

## Аннотация

Спутники все чаще используются для дистанционного зондирования Земли во время стихийных бедствий, что вызывает тревогу в отношении нарушения конфиденциальности данных частных лиц. Несмотря на существование международных документов, таких как *Договор о космосе*, *Принципы, касающиеся дистанционного зондирования Земли из космического пространства,* и *Международная хартия по космосу и крупным катастрофам*, не существует конкретных правил, касающихся неправомерного использования спутников, ведущего к нарушению конфиденциальности. В настоящей статье рассматривается существующее правовое регулирование использования спутников и конфиденциальности данных в Австралии и Индонезии, странах, часто подвергаемых стихийным бедствиям, с целью определения готовности правопорядка разрешать вопросы конфиденциальности данных. Посредством проведения сравнительного анализа обоих правопорядков и международного права в статье подчеркиваются существующие правовые пробелы, которые влияют на применимость и эффективность действия норм. Авторы полагают, что нормы международного права по использованию спутников для дистанционного зондирования, как правило, не имеют обязательной силы и не касаются проблемы нарушения конфиденциальности. В обеих странах также отсутствуют конкретные правовые нормы для устранения нарушений конфиденциальности, вызванных неправильным использованием спутников во время стихийных бедствий. В условиях отсутствия недвусмысленных и конкретных норм международного права авторы считают, что страны могли бы полагаться на национальное право, возможно, частично пересмотрев некоторые его нормы, для решения потенциальных проблем конфиденциальности в связи с развитием возможностей дистанционного зондирования. Установление национальных условий и ограничений на осуществление космической деятельности, включая положения о конфиденциальности, можно было бы обосновать применением статьи VI Договора о космосе, требующей от государств санкционировать и обеспечивать непрерывный надзор за деятельностью неправительственных организаций в космическом пространстве. Существующее космическое законодательство о страховании ответственности также можно было бы расширить, включив в него положения о неприкосновенности частной жизни.

## Ключевые слова

конфиденциальность данных, правовой режим, стихийные бедствия, дистанционное зондирование, неправомерное использование спутников

**Конфликт интересов** Авторы сообщают об отсутствии конфликта интересов.

| | |
|---|---|
| **Финансирование** | Исследование финансировалось APNIC Foundation, номер гранта: F-202206-01436 — Bond University Internet Law Research Clinic: Enhancing the Efficacy of Internet Connectivity Legal Frameworks in the Asia-Pacific Region. |
| **Для цитирования** | Лаваль, Т., Джексон, М., Георгиадес, Е. (2023). Конфиденциальность в эпоху дистанционного зондирования стихийных бедствий в Австралии и Индонезии. *Цифровое право, 4*(2), 15–39. https://doi.org/10.38044/2686-9136-2023-4-2-15-39 |

* Автор, ответственный за переписку

Поступила: 09.06.2023, принята в печать: 27.06.2023, опубликована: 31.07.2023

## Introduction

In November 2022, an earthquake hit Cianjur, West Java, Indonesia, resulting in the death of at least 600 people and causing extensive damage.[1] In a similar vein, several parts of South Australia were affected by a devastating flooding of the River Murray between December 2022 and January 2023, leading to human displacements and significant damage to properties and infrastructure.[2]

Indonesia is located within the ring of fire, a path along the Pacific Ocean that experiences frequent seismic activities leading to earthquakes, volcanic eruptions, and tsunamis (Hakim & Lee, 2020). Consequently, the country is prone to natural disasters, with over 2000 occurrences reported yearly since 2016.[3] Australia on the other hand, has a diverse climate marked by temperature and rainfall variations throughout the year. Significant parts of the country transition between dry and hot conditions characterised by droughts and heatwaves to moist and cooler conditions that often result in flooding.[4] This climate variability is linked to several natural disasters such as bushfires, floods, and heatwaves (Boon, 2013).

During natural disasters, satellites[5] play a vital role in providing essential data and services.[6] They are used in search and rescue efforts to locate individuals who may be stranded or missing,

1 Statista Research Department. (2023, January 17). Number of fatalities due to natural disasters in Indonesia 2016–2022. Statista. https://www.statista.com/statistics/954214/indonesia-fatalities-natural-disasters/#:~:text=In%202022%2C%20there%20were%20around,%2C%20on%20November%2021%2C%202022

2 Some have suggested that this might be the most significant natural disaster in the history of South Australia. See Richards, S. (2023, January 16). *River Murray flood "most significant" natural disaster in SA history. InDaily.* https://indaily.com.au/news/2023/01/16/river-murray-flood-most-significant-natural-disaster-in-sa-history/

3 Statista Research Department. (2023, January 24). *Natural disasters in Indonesia—statistics & facts.* Statista. https://www.statista.com/topics/8305/natural-disasters-in-indonesia/#topicOverview

4 Royal Commission into National Natural Disaster Arrangements. (2020). Royal Commission into National Natural Disaster Arrangements — report. https://naturaldisaster.royalcommission.gov.au/system/files/2020-11/Royal%20Commission%20into%20National%20Natural%20Disaster%20Arrangements%20-%20Report%20%20%5Baccessible%5D.pdf

5 The earthquakes that occurred in certain areas of Turkey and Syria on 6 February 2023 serve as a clear indication of the crucial role of satellites during natural disasters. The activation of the International Charter on Space and Major Disasters facilitated the provision of satellite data (such as images and maps of the impacted areas) to assist in the rescue and recovery operations. *See* Office for Outer Space Affairs UN-SPIDER. (2023, February 7). *Earthquake in Turkey and Syria—International Charter and Copernicus active.* United Nations. https://www.un-spider.org/news-and-events/news/earthquake-turkey-and-syria-international-charter-and-copernicus-active

6 Bronner, E. (2023, February 7). Earthquake in Turkey and Syria: How satellites can help rescue efforts. *The Conversation*. https://theconversation.com/earthquake-in-turkey-and-syria-how-satellites-can-help-rescue-efforts-199357

thereby minimising the disaster's impact.[7] Recently, satellite IoT (Internet of Things), in the form of hundreds or thousands of sensors placed on satellites launched into orbit, is being used as early warning systems to monitor natural disasters such as hurricanes, tornadoes, and earthquakes, and providing critical information to communities at risk.[8] Governments often process the data collected through remote sensing to take necessary actions to detect and mitigate the effects of these natural disasters.[9]

According to Moran (2017)[10], remote sensing involves 'identifying, observing, and measuring an object without coming into direct contact with it.' In other words, it is a means of observing the Earth's surface from space (Nafis et al., 2021). Earth observation satellites launched into orbit carry remote sensors capable of detecting, observing, and collecting information about the Earth's surface and other planetary bodies using various means including satellite imaging (Tronchetti, 2015). This is particularly important as terrestrial communication limitations during natural disasters make the use of satellite technology for emergency communications critical (Page & Besco, 2021). Both private entities and governments are increasingly building or planning to build constellations of Earth observation satellites to conduct remote sensing activities.[11] In 2008, there were only 150 Earth observation satellites in orbit (Tatem et al., 2008). As of 2022, there are over 1,000 Earth observation satellites occupying different orbits.[12] The cost of launching imaging satellites as well as procuring high-resolution satellite images capable of remote sensing is constantly decreasing.[13]

Historically, Earth observation satellites were placed in the geosynchronous equatorial orbit (GEO), which is about 36,000 km above Earth's surface.[14] Due to the distance from Earth, images captured from GEO were of low quality (Emery & Camps, 2017). However, with the continuous advancements in technology, Earth observation satellites are now being placed in the low Earth orbit (LEO), which is much closer to Earth's surface (Emery & Camps, 2017). This allows for higher spatial resolution images to be captured, as the closer a satellite is to Earth's surface, the better the resolution of the images that can be captured (Emery & Camps, 2017). This has led to diverge opinions as to how different countries view remote sensing activities. Countries that actively engage in remote sensing believe that collection and dissemination of satellite data have significant international benefits (Mosteshar, 2016). Others, especially developing countries, hold the view that the use of satellites

7 Fair Tech Institute. (2020). *The Role of Satellite Communications in Disaster Management.* https://accesspartnership.com/wp-content/uploads/2022/03/The-Role-of-Satellite-Communications-in-Disaster-Management.pdf

8 Inmarsat. (2021, April 22). *Satellite-based monitoring to reduce impact of natural disasters.* [Press Release]. https://www.inmarsat.com/en/news/latest-news/government/2021/satellite-monitoring-impact-natural-disasters.html

9 Fair Tech Institute. (2020). *The Role of Satellite Communications in Disaster Management.* https://accesspartnership.com/wp-content/uploads/2022/03/The-Role-of-Satellite-Communications-in-Disaster-Management.pdf

10 Moran A. (2017, August 16). Remotely Sensing Our Planet. NASA. https://svs.gsfc.nasa.gov/30892

11 These satellites are equipped with advanced high precision sensors capable of capturing and processing high-definition images of the Earth's surface. *See* Beam, C. (2019, June 26). Soon, satellites will be able to watch you everywhere all the time: Can privacy survive? *MIT Technology Review.* https://www.technologyreview.com/2019/06/26/102931/satellites-threaten-privacy/

12 Thorpe, E. (2022, March 5). *Earth Observation Satellites Imagery: Types, Application, And Future Trends*. Orbital Today. https://orbitaltoday.com/2022/03/05/earth-observation-satellites-imagery-types-application-and-future-trends/

13 Chow, D. (2022, April 9). To cheaply go: How falling launch costs fueled a thriving economy in orbit. *NBC News*. https://www.nbcnews.com/science/space/space-launch-costs-growing-business-industry-rcna23488

14 Jagula, D. (2022, February 19). *Satellite imagery for everyone.* IEEE Spectrum. https://spectrum.ieee.org/commercial-satellite-imagery

by sensing countries which extends to obtaining data about the territory and natural resources of another State violates their sovereignty, and such activities should require the prior consent of the Sensed state (Mosteshar, 2016).

Thus, despite the immense benefits of remote sensing activities carried out using satellites, they are also prone to misuse, particularly during natural disasters. With the constant advancements in remote sensing capabilities (Ito, 2011; Sitanggang, 2018), the potential for the misuse of satellites resulting in privacy breaches have increased. Misuse can occur when monitoring places, objects, or people without prior notification or authorisation. Any information collected through satellite imaging can be misused through the improper dissemination of data or reaching false conclusions based on wrong data interpretation.[15]

Consequently, satellites' misuse can result in privacy breaches when collecting data through remote sensing activities. Singh et al. (2012) highlight concerns about the commercialisation of remote sensing using satellite imagery and the potential for abuse. Santos and Rapp (2019) argue that as low-cost commercial satellite systems become operational, high-resolution imagery will become a regular part of end-user products and information services. Accordingly, advancements in the resolution capacity of remote satellite technology will inevitably raise debates on the infringement of citizens' privacy, as monitoring can now be done from continents away without the need for installed cameras.[16] Singh et al. (2012) further suggest that 'the rapidly improving resolution capacity coupled with the growth in nanotechnology could enable live recording instead of imagery in the near future and we are left to imagination to perceive the threat posed by unfettered usage of remote sensing satellites.'

Although there are international frameworks such as the *Remote Sensing Principles*[17] and *Disasters Charter*,[18] as discussed later, they are generally not legally binding and do not provide specific rules for addressing privacy breaches that occur during satellite-based remote sensing activities, particularly in natural disasters situations (de Beer, 2020; Sitanggang, 2018).

Consequently, this article, which consists of two parts, focuses on the intersection of privacy protection and satellite use during natural disasters. The first part clarifies the specificity of collecting and processing personal data during natural disasters by distinguishing it from general electronic surveillance. It discusses the unique challenges posed by disaster situations such as the urgency and necessity of data collection, the potential for large scale data breaches, and the increased vulnerability of affected individuals. An analysis of how the circumstances of natural disasters can impact privacy rights, including issues of consent, data security, data retention, and the potential for re-identification of anonymised data is also undertaken.

The second part provides a comparative analysis of the relevant provisions of Australian and Indonesian law pertaining to use of satellite, particularly for remote sensing, and privacy

---

15 Beam, C. (2019, June 26). Soon, satellites will be able to watch you everywhere all the time: Can privacy survive? *MIT Technology Review*. https://www.technologyreview.com/2019/06/26/102931/satellites-threaten-privacy/

16 Between 2007 and 2017, India launched CARTOSAT-2, a series of remote sensing satellites with spatial resolution of less than a meter. To illustrate the extent of these sort of resolution capabilities, the satellite imagery collected by these satellites are capable of being used to detect the model and make of a car on Earth. *See* (Singh, 2012).

17 *The Principles Relating to Remote Sensing of the Earth from Outer Space*, UN GA Res 41/65 — adopted on 3 December 1986. See generally the different principles, especially Principle I that defines raw data, processed data and analysed data, Principle XI that envisages that 'Remote sensing shall promote the protection of mankind from natural disasters.'

18 *Charter on Cooperation to Achieve the Coordinated Use of Space Facilities in the Event of Natural or Technological Disasters*, opened for signature 20 October 2000.

considerations during natural disasters.[19] It also analyses relevant international instruments related to remote sensing, natural disasters, and privacy, evaluating their applicability and effectiveness in addressing privacy issues arising from the use of satellites for remote sensing during natural disasters. Through this, gaps are identified in the existing legal frameworks and suggestions proffered for potential improvements that can be explored to address the specific privacy issues arising from advancing remote sensing capabilities.

## Part I — Handling of personal data during natural disasters

### Contrasting personal data collection during natural disaster and surveillance

To better understand the focus of this article on privacy implications arising from collection and processing of personal data using remote sensing capabilities during natural disasters, an appropriate starting point would be to distinguish this process from general electronic surveillance.

The first differentiating factor pertains to the purpose of data collection. During natural disasters, data is typically collected for emergency management, disaster relief, and recovery activities (Yu et al., 2018). In contrast, electronic surveillance is often carried out for national security, economic stability, or other social benefits.[20] Consequently, the legal implications and law governing both activities differ considerably. Where they exist, legal frameworks relating to data collection and processing during natural disasters are generally designed to ensure the safety and well-being of individuals.[21] These frameworks, such as the provision of Part VIA of the Privacy Act (Cth) discussed later, may specify the types of data that can be collected, the purposes for which it can be used, and the specific safeguards required to protect privacy and data security. They may also include provisions for securing and preventing unauthorised access and misuse of the collected data. On the other hand, electronic surveillance is often governed by wiretapping statutes that regulate the interception of electronic communications for law enforcement or national security purposes (National Research Council, 1996). These laws, such as the Telecommunications (Interception and Access) Act 1979 (Cth), are typically employed for intercepting and retaining communications data, especially during intelligence operations.

Another important distinction between data collection during natural disasters and surveillance is the impact on privacy. During natural disasters, data collection and processing may involve accessing social media posts, health records, and other personal information (Kuner & Marelli, 2020). As earlier alluded to, this is primarily done to provide emergency services and support, rather than for surveillance purposes. However, general electronic surveillance can significantly impact a broad spectrum of rights, including privacy. Some argue that surveillance is inherently harmful, as Quentin Skinner explains: "I think it is very important that the mere fact of there being surveillance takes away liberty… it is true that my privacy has been violated if someone is reading my emails without my knowledge… my liberty is also being violated, not merely by

[19] While the emphasis for potential misuse of satellites in this article pertain to privacy breaches in the context of natural disasters, it should be noted that the misuse of satellites also applies in other contexts.

[20] Lee, N.T., & Chin, C. (2022). *Police surveillance and facial recognition: Why data privacy is imperative for communities of color.* Brooklings. https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/

[21] United Nations Office for Disaster Risk Reduction. (2015). Sendai Framework for Disaster Risk Reduction 2015-2030. United Nations. https://www.undrr.org/quick/11409

the fact that someone is reading my emails but also by the fact that someone has the power to do so should they choose".[22]

## Challenges of data collection in relation to privacy during natural disasters

Despite the primarily beneficial nature of data collection during natural disasters, there are unique challenges and considerations related to privacy.

One such challenge is the urgency and necessity of data collection. During natural disasters, there is often an urgent need to gather data to support emergency management, particularly in order to deliver health services, relief materials, and carry out recovery activities (Kuner & Marelli, 2020). For example, the activation of the Disaster Charter is available year-round, and activations typically occur within 10 days of a disaster.[23] Member agencies prioritise providing satellite data to requesting countries as quickly as possible to aid in disaster management and recovery. Therefore, obtaining informed consent from disaster victims becomes impractical in many cases. This impacts one of the salient principles of data protection — consent as a lawful basis for processing personal data. In distressing situations, it is questionable to consider any 'consent' given by someone in need of humanitarian assistance as truly 'freely' given (Kuner & Marelli, 2020). Moreover, during natural disasters, individuals are more likely to share personal information in exchange for emergency support (Sheinidashtegol et al., 2019), which increases their vulnerability and the risk of privacy breaches. Individuals affected by natural disasters may be unaware of how their personal data is collected, processed, or used, potentially breaching the provisions of some data privacy legislation (*Privacy Act* 1988 (Cth), APPs 3, 6, 11).

Another challenge relates to data retention. A common requirement during data collection and processing is the obligation to delete or anonymise data once the purpose for which it was collected has been served. However, during a natural disaster event, there might be a need for data to be retained longer than would be necessary in a non-emergency situation (Sanfilippo et al., 2020). The risk of privacy breaches, therefore, heightens especially if the data is not securely stored and is subsequently accessed by unauthorised persons. While data minimisation, which involves collecting only the minimum amount of personal data necessary for a specific purpose, is considered a useful strategy (Qu et al., 2019), it does not completely eliminate the risk associated with privacy breaches.

Furthermore, there remains an associated risk of data breaches, including cyber-attacks on data collected during natural disasters. Anonymisation is often proposed as a preventive measure to protect individuals' privacy by removing personally identifiable information from datasets (Nishara & Pandey, 2015). In the context of natural disasters, the expectation is that once data is anonymised, the personal information of individuals is safeguarded while allowing for data collection and analysis. However, the risk of re-identifying anonymised data is not completely eliminated, especially when such data is combined with other datasets.[24]

---

[22] Marshall, R., & Skinner, Q. (2013, July 26). Liberty, liberalism and surveillance: A historic overview. *OpenDemocracy*. https://www.opendemocracy.net/en/opendemocracyuk/liberty-liberalism-and-surveillance-historic-overview/

[23] Office of Outer Space Affairs. (n.d.). *International Charter Space and Major Disasters.* United Nations. Retrieved June 7, 2023. https://www.un-spider.org/international-charter-space-and-major-disasters

[24] Tyrrell, J. (2023, February 2). *Re-identification risks: Can data ever be fully anonymized?* T_HQ: Technology and business. https://techhq.com/2023/02/re-identification-risks-can-data-ever-be-fully-anonymized/

## Part II — National and International legal regime on remote sensing, natural disasters and privacy

Resulting from the analysis in the previous part, it becomes important to probe the question of whether there exist adequate provisions, generally under international law, and specifically under Australian and Indonesian law to address the potential for privacy breaches that may arise when carrying out remote sensing activities during natural disasters.

### Landscape of national Legal framework for the regulation of LEO satellites

The advancement in satellite technology is facilitating the deployment of constellations of satellites in the low earth orbit (LEO). These satellites are used for various purposes, including for remote sensing. It therefore becomes important to commence the discussion in this section with an overview of the current legal framework in Australia and Indonesia which relates to the regulation of LEO satellites.

#### *Australia*

In Australia, space activities are primarily regulated pursuant to the *Space Act,*[25] and the *Telecommunications Act*.[26] It is a State Party to all the major international treaties governing space, including the *Outer Space* Treaty.[27] The Australian Space Agency (ASA) regulates Australian space activities, while the Australian Communications and Media Authority (ACMA) regulates communications and media services. ACMA also serves as the Australian administration for the International Telecommunications Union's international process of managing frequencies for satellite communications.[28]

Under Section 42 of the *Telecommunications Act*, a carrier license is required for any person who uses a network unit to supply a carriage service to the public. A network unit includes a designated radiocommunications facility that uses different means, including satellites, to supply carriage services between different points in Australia. If such operator requires the use of radio frequency spectrum, a radiocommunications licence must be granted,[29] as well as other necessary authorisations to set up and operate a satellite network.[30]

Section 18 of the *Space Act* contains regulatory and licensing provisions relating to launch facilities, launching, and returning of space objects (which encompasses satellites),[31] as well as liability for damage by space objects. By virtue of Sections 11, 12, 15, 18 and 28 of the *Space Act*, a licence is

25 Space (Launches and Returns) Act, 2018 (Cth).

26 Telecommunications Act, 1997 (Cth).

27 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (GA Res 2222 (XXI), annex) — adopted on 19 December 1966, opened for signature on 27 January 1967, entered into force on 10 October 1967.

28 Australian Communications and Media Authority. (2012). *Australian procedures for the coordination and notification of satellite systems.* Australian Government. https://www.acma.gov.au/sites/default/files/2019-11/aust_procedures-coordination_notification_of_satellite_systems%20pdf.pdf

29 *See generally* Chapter 3 of the Radiocommunications Act, 1992 (Cth).

30 Australian Communications and Media Authority. (n.d.). *Set up and operate a new satellite network*. Retrieved June 7, 2023. https://www.acma.gov.au/set-and-operate-new-satellite-network

31 Although satellites are not explicitly mentioned under the *Space Act,* Section 8 defines 'space objects' to mean 'any object the whole or a part of which is to go into or come back from an area beyond the distance of 100 km above mean sea level.' This definition captures satellites within its scope.

generally required to operate a launch facility in Australia, and a launch permit is required to launch and return a space object from and to a facility or area in Australia. Australian nationals require an overseas payload permit and return authorisation to launch and return space objects respectively from and to a place outside Australia pursuant to Sections 14, 15A, 46B, and 46L of the *Space Act*. Since satellites fall under the definition of space objects, the regulatory and licensing provisions under the *Space Act* also apply.

As part of the licensing process, Section 22, 56, and 102 of the *Space (Launches and Returns) (General) Rules* requires an applicant to submit a technology security plan that includes procedures for preventing unauthorised access to the technology and ensuring cybersecurity. However, while the plan requires that the cybersecurity of the technology used in relation to the launch and return of a space object be safeguarded, it does not stipulate any standards for safeguarding these space objects against cyberattacks during launch and return. This is particularly concerning since remote sensing satellites launched into orbit can capture high-resolution images of Earth's surface, including information that can be used to identify individuals (Singh et al., 2012). As would be discussed in the later part of this article, the *Privacy Act*[32] requires personal information to be safeguarded against potential unauthorised use, loss, disclosure, alteration, or access.

Although the above provisions of the *Space (Launches and Returns) (General) Rules* relate to safeguards during launch and return of satellites, it is nonetheless useful to highlight the connection with the *Privacy Act* as explained above. To put in context, there have been instances when sensitive satellite infrastructure of the Australian government or private entities have been subject to sophisticated cyber-attacks (Verco, 2021). For instance, between 2015 and 2016, the systems of the Australian Bureau of Meteorology were subjected to cyber-attacks.[33] Besser & Sturmer (2016) suggest that the true targets for this attack may have been the defence assets linked to the Bureau of Meteorology and its 'vast data collection capabilities.'[34] It is evident that satellites are becoming increasingly susceptible to cyberattacks that can lead to privacy breaches, and with the increasing participation of governments, private entities, and individuals in space activities, it becomes important that these satellites are adequately protected from cyber-attacks (Housen-Couriel, 2016).

### *Indonesia*

Indonesia, as a State Party to the *Outer Space Treaty*, has an obligation to regulate space activities within its territory (von der Dunk, 2002). To meet this obligation, Indonesia has specific frameworks for regulating space activities and the use of satellites for communications services. The primary laws in this regard are the *Law on Telecommunication*[35] and the *Space Law*.[36]

Telecommunications is defined under Article 8 of the *Law on Telecommunication* as 'any emission, transmission, and/or reception of information in the forms of signs, signals, writings, images, voice and sound through wire, optic, radio, or other electromagnetic systems.' This definition is broad

[32] Privacy Act 1988 (Cth).

[33] Uhlmann, C. (2015, December 2). *China blamed for "massive" cyber attack on Bureau of Meteorology computer.* ABC News. https://www.abc.net.au/news/2015-12-02/china-blamed-for-cyber-attack-on-bureau-of-meteorology/6993278

[34] Besser, L., & Sturmer, J. (2016, August 29). *Government computer networks breached in cyber attacks as experts warn of espionage threat.* ABC News. https://www.abc.net.au/news/2016-08-29/chinese-hackers-behind-defence-australe-security-breaches/7790166; 1. BBC News. (2016, October 12). *Australia weather bureau hacked by foreign spies, says report*. https://www.bbc.com/news/world-australia-37615645

[35] Law No. 36 of 1999 on Telecommunication.

[36] Law No 21 of 2013 Concerning Space Activities.

enough to cover different mediums of transmission, including satellites and the different uses they can be put to.

Due to its unique geography (Nafis et al., 2021), Indonesia's telecommunications system relies heavily on communications satellites (Sastrawidjaja & Suryanegara, 2018), which transmit and receive information through radio frequencies (Sitanggang, 2018). Communications satellites are essential to many services including remote sensing activities, mobile communication services, broadcasting, disaster management, and weather forecasting (Supancana, 2006). Whilst Indonesia uses foreign satellites, it also has its own system of communications satellites (Nafis et al., 2021) currently made up of nine (9) satellites.[37] Pursuant to Article 33 of the *Law on Telecommunication*, the use of radio frequency spectrum and satellite orbit is a licensable telecommunication undertaking.

Furthermore, Article 6 of the *Law on Telecommunication* empowers the Minister of Communications and Informatics to regulate telecommunications in Indonesia, including the use of satellites for communications services. While the National Institute of Aeronautics and Space (LAPAN) has been carrying out supervisory functions over all space activities in Indonesia pursuant to Article 38(4) of the *Space Law*. Despite not being specifically mentioned under the *Space Law*, LAPAN has been undertaking that responsibility as the existing national space agency since its establishment in 1963.[38] However, with the creation of the National Research and Innovation Agency (BRIN), LAPAN's role as the country's space agency is being transferred to BRIN (Nugraha et al., 2022). A thorough reading of Article 1 and 5 reflects that the *Space Law* applies to all space activities occurring within the territory or jurisdiction of Indonesia, all space activities occurring on behalf of or otherwise attributable to Indonesia, or space activities conducted by Indonesian citizens or Indonesian legal entities with a license to undertake space activities.

To regulate space activities, Article 41 and 42 of the *Space Law* requires entities to obtain a license before engaging in space activities. Additionally, Article 71 of the *Space Law* mandates that all space objects, including satellites, must be registered with the Indonesian government, providing sufficient information on their orbital parameters, function, purpose, and launching entity. It clarifies that registration is necessary to ensure open information and must be published and easily accessible. Operators of space activities are prohibited from placing, orbiting, or operating nuclear weapons or other weapons of mass destruction (Supancana, 2015). Furthermore, operators must ensure the protection and preservation of the environment, including any activities that may contaminate Earth's environment (Froehlich & Seffinga, 2018). Indonesia recognises the involvement of private entities in the space segment, and the *Space Law* aims to ensure that all space activities, including commercialisation, are carried out in an orderly manner and for the benefit of humankind (Froehlich & Seffinga, 2018).

## International Legal framework related to use of LEO satellites for remote sensing during natural disasters

The use of outer space for various activities, including remote sensing using satellites, increased significantly after the end of the Cold War (Zunnuraeni et al., 2020). To guide the carrying out of these

[37] Mulyadi. (2016, September 6). *Indonesian Satellite Service Regulatory Framework*. ITU International Satellite Symposium 2016, Bali. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2016/Sep-ISS2016/Presentation/ITU%20International%20Satellite%20Symposium%202016%20-%20Indonesia.pdf

[38] Mardianis. (2014, March 24). *The Indonesian Space Act NO. 21/2013*. Fifty-third session of UNCOPUOS Legal Subcommittee, Vienna. https://www.unoosa.org/pdf/pres/lsc2014/tech-02E.pdf

activities, the *Remote Sensing Principles*[39] were passed in 1986 as a resolution of the United Nations General Assembly (Gummadi & Gupta, 2022). The Principles were adopted as a compromise between the conflicting views of sensed States and sensing States (Mosteshar, 2016). While sensing States believe that the data collected during remote sensing are of immense international benefits, most sensed States believe that such activities impede on their territorial sovereignty (Mosteshar, 2016).

In relation to natural disasters, Principle XI of the *Remote Sensing Principles* provides that 'remote sensing shall promote the protection of mankind from natural disasters.' According to Dodge (2014), this Principle is the 'clearest statement in international law that space-based Earth observation is to be used to protect human life from the effects of natural disasters.' However, its provisions only serve as principles and are not legally binding on States, even if those States voted in favour of them and agreed to them (von der Dunk, 2002). Furthermore, it failed to clearly address issues such as liability and privacy considerations when conducting remote sensing. It also falls short in ensuring satellite data obtained during remote sensing comply with privacy laws under national and international laws (Gummadi & Gupta, 2022), which is relevant in the context of remote sensing during natural disasters.

The *Disaster Charter* is another framework established to provide guidelines for use of remote sensing technology during natural disasters. The *Disaster Charter* was created in 1999 by the Centre National D'Etudes Spatiales[40] and the European Space Agency during the Unispace III conference held in Austria, but officially came into operation on 20 October 2000 after the Canadian Space Agency joined.[41] Currently, it consists of 17-member space agencies who jointly provide free satellite imagery over the disaster areas as soon as the charter is activated.[42] It serves as a framework through which its members collaborate to respond to major natural disasters around the world using satellites. These member space agencies provide fast access to satellite data to aid disaster management as soon as it is triggered by any of the authorised users.[43]

One main distinction between the *Remote Sensing Principles* and the *Disaster Charter* is that while parties to the former are States, members of the latter are space agencies and space systems operators which include private entities (Mosteshar, 2016). Accordingly, it fosters collaboration among space agencies, to share their space facilities in managing major natural or man-made disasters (Mosteshar, 2016). This cooperation ensures that necessary assistance, through the provision of

[39] The Remote Sensing Principles comprise 15 non-binding but politically relevant principles that guide how UN member states conduct remote sensing activities. It defines what remote sensing is and attempts to establish a legal framework prescribing how collection and dissemination of remote sensing data should be carried out while also restating general principles of international law contained under the Outer Space Treaty. *See* (Gummadi & Gupta, 2022).

[40] The French national space agency.

[41] Bally, P., Boubila, F., Viel, M., Jutz, S., Cheli, S., & Briggs, S. (2010). *In Action Around the World: The International Charter 'Space and Major Disasters' (Bulletin No. 143).* European Space Agency. https://earth.esa.int/eogateway/documents/20142/37627/In-action-around-the-world-the-International-Charter-Space-and-Major-Disasters.pdf

[42] Bronner, E. (2023, February 7). Earthquake in Turkey and Syria: How satellites can help rescue efforts. *The Conversation*. https://theconversation.com/earthquake-in-turkey-and-syria-how-satellites-can-help-rescue-efforts-199357

[43] Registration to become an authorised user is open to the disaster management authorities of all countries in the world, provided they meet the prescribed criteria stipulated under the Charter. As of February 2022, national users from 67 countries have been designated authorised users. In addition, 15 international organisations, including the United Nations Office of Outer Space Affairs (UNOOSA), can trigger the Charter system, thereby ensuring all countries of the world can benefit from the Charter, regardless of their registration status. See The International Charter Space and Major Disasters Executive Secretariat. (n.d.). *How to become an authorised user.* Retrieved June 7, 2023. https://disasterscharter.org/web/guest/how-to-register-as-a-user

satellite data collected, is extended to countries or communities that are exposed to an imminent risk, or that have already been affected by such disasters (Mosteshar, 2016).

Since 2000, the *Disaster Charter* has been activated 798 times in 131 countries (Mosteshar, 2016)[44]. However, it is a voluntary agreement among its members and is not legally binding (Zollner, 2018). Like the *Remote Sensing Principles*, it does not create any obligations but serves as a mechanism to provide information and other assistance (Mosteshar, 2016). While the *Disaster Charter* aims to facilitate the exchange of satellite data between space agencies and disaster management organisations to support response and recovery efforts (Zollner, 2018), it does not address issues regarding the use of satellites that may result in privacy breaches. Arising from the shortcomings of these international frameworks, the next section will examine the international law regime concerning privacy, after which an evaluation of the national legislation in Australia and Indonesia that deal with data privacy will be carried out.

## Legal framework on data privacy

As noted previously, satellites play a vital role in supporting rescue and recovery efforts during natural disasters. Nevertheless, it is also important to ensure privacy rights are protected while using satellites to collect data, especially when the data collected can potentially be used to identify individuals. Satellite technologies gather different types of data, and as technology advances, it is not far-fetched that information capable of being used to identify individuals can be obtained during remote sensing activities. User identity has been identified as one of the important areas of concerns while discussing different countries approaches to remote sensing regulation (Mosteshar, 2016). In light of this, it is essential to ensure that privacy considerations are not overlooked when examining issues of satellite sensed data under national legislation.[45] Therefore, it is important, in this context, to assess the existing legal frameworks pertaining to data privacy first under international law, and then under Australian and Indonesian law.

## International law regime related to data privacy

The characteristics of remote sensing make it probable that technologies used to carry out these activities would have privacy ramifications. The applicability of privacy law in this context stems from the understanding that while the sensing activity itself takes place in space through Earth observation satellites, the information gathered by these satellites relate to activities and information on Earth (Freeland & Ireland-Piper, 2022). Thus, an Earth observation satellite used in obtaining satellite imagery of areas where a natural disaster has occurred would essentially be capturing data relating to the disaster areas, and not 'space' data. This presents an opportunity to examine these activities within the framework of existing international law to assess how effectively they address privacy concerns during remote sensing.

In this respect, the Universal Declaration of Human Rights (UDHR),[46] International Covenant on Civil and Political Rights (ICCPR)[47] and the International Covenant on Economic Social and Cultural

[44] *See also* The International Charter Space and Major Disasters Executive Secretariat. (n.d.). *How to become an authorised user.* Retrieved June 7, 2023. https://disasterscharter.org/web/guest/how-to-register-as-a-user

[45] Williams, M. (2006). *Legal aspects of the privatization and commercialization of space activities, remote sensing, and national space legislation.* International Law Association. https://ila.vettoreweb.com/Storage/Download.aspx?DbStorageId=1044&StorageFileGuid=2dc0ec9c-0fb5-4b9d-b12d-20f82ec3e4ae

[46] Universal Declaration of Human Rights, GA Res 217A (III), UN Doc A/RES/217(III) (10 December 1948)

[47] International Covenant on Civil and Political Rights, UN GA Res 2200A (XXI) — adopted 16 December 1966, opened for signature 19 December 1966, entered into force 23 March 1976.

Rights (ICESCR)[48] are three key international covenants that form the basis of human rights provisions in various international, regional, and national legal frameworks.

Interestingly, the proximity in the dates the ICCPR and ICESCR were adopted (16 December 1966) and when the first major international treaty governing space — *Outer Space Treaty* — was adopted (19 December 1966) cannot be seen as a mere coincidence. Reflecting on the provisions of Article III of the *Outer Space Treaty* shows that its intention is to be read in consonance with other international law. Specifically, it provides that 'State Parties to the Treaty shall carry on activities in the exploration and use of outer space... in accordance with international law...in the interest of maintaining international peace and security and promoting international co-operation and understanding.' The inclusion of the phrase 'in accordance with international law' in this provision, as well as in Article I, can be interpreted as a deliberate consideration of existing international law such as UDHR as well as concurrent negotiations that were being carried out in respect of other international legal framework, such as the ICCPR, at that time.

Furthermore, the provision of Article III of the *Outer Space Treaty*, when read in conjunction with Articles I and II, establishes a dual concept. Firstly, it guarantees the freedom of every country to engage in exploration activities in outer space. Secondly, it prohibits any nation from asserting territorial sovereignty over any part of outer space. As remote sensing is an activity conducted from outer space, it falls within the scope of the aforementioned freedom (von der Dunk, 2013: 2). This is further buttressed by the right to freedom to seek, receive, and impart information through any media or frontier, pursuant to the provisions of the UDHR and ICCPR.[49] Since remote sensing is used to seek and receive information about activities taking place on the Earth's surface, it aligns with these rights.

The right to privacy, guaranteed under the UDHR and ICCPR, is a competing right that should be considered in the context of remote sensing. Article 12 of the UDHR states that 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour or reputation.' A similar provision is found in Article 17 of the ICCPR. However, these privacy provisions are drafted in broad terms and do not specifically address the privacy concerns that may arise from remote sensing activities. Additionally, while Greenwood et al. (2017)[50] argues that data privacy during humanitarian crises should align with international human rights and humanitarian law and standards, there is no established internationally recognised humanitarian standard for data privacy in such situations.[51] Consequently, these instruments do not sufficiently accommodate or regulate data privacy issues in the context of remote sensing during natural disasters.

On one hand, the *Outer Space Treaty* grants each nation the freedom to conduct activities in outer space, a freedom extended to the freedom to seek, receive, and impact information through any frontier (in this case, remote sensing) under Article 19 of both the UDHR and ICCPR. This freedom is not subject to territorial jurisdiction in outer space. On the other hand, the UDHR and ICCPR guarantee individuals' right to privacy. These two perspectives create a potential conflict that requires a balancing act, one that is not clearly addressed under international human rights law.

---

48 International Covenant on Economic, Social and Cultural Rights, UN GA Res 2200A (XXI) — adopted 16 December 1966, opened for signature 19 December 1966, entered into force 3 January 1976.

49 Article 19 UDHR and Article 19 ICCPR.

50 Greenwood, F., Howarth, C., Poole, D. E., Raymond, N. A., & Scarnecchia, D. P. (2017). *The signal code: A human rights approach to information during crisis*. Harvard Humanitarian Initiative. https://hhi.harvard.edu/sites/hwpi.harvard.edu/files/humanitarianinitiative/files/signalcode_final.pdf?m=1607469621

51 Halle, E. (2018). International human rights framework to disaster management. https://dx.doi.org/10.2139/ssrn.3287849

It is worth noting that the *Outer Space Treaty* lacks specific rules or guidance on how the freedom to conduct activities in outer space may be limited, particularly regarding potential privacy concerns that may arise during remote sensing. Some argue that this lack of specificity could be attributed to the fact that privacy concerns resulting from remote sensing were not prominent when the *Outer Space Treaty* was adopted, as high-resolution remote sensing technology did not exist at that time (von der Dunk, 2013: 7). Moreover, the primary focus of the United Nations at that time was to create guiding rules for the exploration of outer space for peaceful purposes, and for the benefit of every nation, in an era when the two major space faring nations — US and USSR — were increasingly developing their space technology capabilities (Freeland and Pacujlic, 2018).

As a result, von der Dunk (2013) suggests that in the absence of any general international law agreements or customary international law addressing privacy concerns, which could be incorporated into the scope of the *Outer Space Treaty* under Article III, it is the responsibility of individual countries to establish safeguards within their national laws to limit the seemingly unfettered freedom to conduct remote sensing activities that the *Outer Space Treaty* or any other international law has not limited, in light of privacy concerns. This is so as Article VI of the *Outer Space Treaty* imposes international responsibility on individual countries for their own outer space activities, as well as those of non-governmental entities under their jurisdiction. Accordingly, countries have the authority to regulate private space activities, including the power to prohibit them altogether or require compliance with specific national laws protecting privacy of individuals and entities (von der Dunk, 2013).

With this in mind, the next section examines the legal framework on data privacy in Australia and Indonesia to assess the adequacy of these laws in addressing privacy concerns arising from remote sensing activities.

## Legal framework on data privacy in Australia and Indonesia

### *Australia*

The main data privacy framework in Australia is the *Privacy Act*.[52] One of its objects under Section 2A is 'to provide the basis for nationally consistent regulation of privacy and the handling of personal information.' Personal information is defined in Section 6 as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.' Georgiades (2020) opines that the scope of the *Privacy Act* applies to personal information recorded and captured digitally.

As has been previously discussed, during a natural disaster, personal information collected by satellites can result in misuse. For example, satellites can capture very high-resolution images when used for remote sensing (Kaku, 2019). The capturing of such images has potential ramifications for people's privacy because such images can include information that can identify an individual. Consequently, the processing of the information captured would need to comply with the *Privacy Act* as it falls within the scope of collecting, storing, and monitoring of data. Although the Act does not explicitly mention satellites, it applies to data collected by various means, which includes satellites.

[52] Privacy Act, 1988 (Cth). Australia currently lacks a legal framework specifically regulating the use of remote sensing technology to prevent data privacy breaches. Nonetheless, it is important to examine the existing data privacy framework, to determine if they are adequate in preventing misuse during natural disasters. *See* The University of Adelaide. (2019). *Laws applicable to remote sensing*. Australian navigational guide explaining laws for space. https://spacelaws.com/articles/laws-applicable-to-remote-sensing-activities/

Therefore, compliance with the provisions of the *Privacy Act* is required when collecting personal information.

The *Privacy Act* is applicable to and imposes obligations on APP entities. Section 6 defines an APP entity to be an agency or an organisation. An agency includes *inter alia,* a Minister, a Department, a body, or tribunal established for a public purpose under a Commonwealth, State, or Territory law. An organisation is defined under Section 6C to include an individual, body corporate, partnership, unincorporated association, or trust. However, State or Territory authorities, political parties, and small business operators are not considered organisations.[53]

An important provision of the *Privacy Act* is Section 5B that deals with extra-territorial applicability of the *Privacy Act*. Section 5B(2) and (3) extends the applicability of the *Privacy Act* to organisations or small business operators with an 'Australian link'. Examples of Australian link under Section 5B(2) include where an organisation is incorporated or forms a partnership in Australia. By virtue of Section 5B(3), even where an organisation or small business operator does not fall under any of the above listed entities, it would still be considered to have an Australian link if it carries on business in Australia. The term 'carries on business in Australia' has generally been viewed as two elements that are connected; however, they can be considered separately (*Luckins v Highway Motel (Carnavon) Pty Ltd*, 1975; *Bray v F Hoffman-La Roche Ltd*, 2002; *ASIC v Active Super (No 1)*, 2012).

In a recent ruling, the full bench of the Federal Court interpreted 'carries on business in Australia' to encompass foreign organisations that collect or hold personal information of persons located in Australia, notwithstanding that such entities do not have physical assets in Australia (*Facebook v. AIC*, 2022). Thus, merely collecting or handling personal information of any person located in Australia will suffice to make an entity subject to the provisions of the *Privacy Act* ( Svantesson, 2014, 2015)[54]. This means that as long as satellites are used to carry on business which involves collection, holding or storing of personal information of any person located in Australia, the *Privacy Act* will apply.

The *Privacy Act* also protects biometric information which is categorised under Section 6 as sensitive information. While Section 6 does not include a list of information that could be considered biometric information, the Office of the Australian Information Commissioner lists attributes such as an individual's face, iris, fingerprint, palm, voice, and signature, as constituting biometric information.[55] This information can be collected with the relevant individual's consent, except when authorised by law or to prevent a serious threat to life, health, or safety (*Privacy Act 1988* (Cth) APPs 3.3, 3.4). In this regard, Maniadaki et al. (2021) argues that 'the application of facial recognition or big data analytical software in data collected by remote sensing technology puts in danger the protection of personal data when it constitutes the process of personal data.'

Whilst satellite imagery is useful for weather monitoring and defence intelligence, in the event of natural disasters, the use of high-resolution satellite imagery create challenges for data protection (Coffer, 2020). In addition to geographical locations and interactive maps, there are now facial recognition technologies causing more concern for personal data collection (Maniadaki et al., 2021). Since satellites can capture higher resolution images, it is crucial to comply with the requirements set

---

[53] Office of the Australian Information Commissioner. (n.d.). State and territory privacy legislation. Retrieved June 7, 2023. https://www.oaic.gov.au/privacy/privacy-in-your-state#:~:text=Queensland%2C%20the%20Northern%20Territory%20and,public%20sector%20health%20service%20providers

[54] *See also* Ganko, M. (2022, December 15). Privacy is not dead in Australia; it's diffusing. *Iapp*. https://iapp.org/news/a/privacy-is-not-dead-in-australia-its-diffusing

[55] Office of the Australian Information Commissioner. (n.d.). *Biometric scanning.* https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/biometric-scanning

out in the *Privacy Act* if satellite imagery includes biometric information. Of importance is Schedule 1 of the *Privacy Act* which contains 13 Australian Privacy Principles (APPs) that govern the utilisation, exposure, and safeguarding of gathered data (Alazab et al., 2021; Daly, 2018; Sainty & Rowe, 2020). Among these principles, APP 4, 6, 8, and 11 may be applicable to the collection, use, and disclosure of data gathered by satellites in different contexts including remote sensing activities. The relevant APPs are examined subsequently.

APP 4 provides the way in which an entity is to handle unsolicited personal information. Unsolicited personal information is described under Schedule 1 to mean personal information received by an APP entity without it taking active steps to collect such information. This APP is relevant to satellites since they can often inadvertently collect data about an individual. This could also lead to unauthorised surveillance or uncontrolled data generation and use (Caron et al., 2016). If unsolicited data is obtained in the process of carrying out remote sensing activities, the APP entity must ascertain whether this type of data can be collected under APP3. According to APP 3, data can only be collected by an agency or organisation if it is reasonably necessary or directly related to the agency or organisation's functions and activities. If the APP entity determines that it can collect the type of data under APP 3 or data collected is contained in a Commonwealth Record, then the APP entity is not mandated to destroy or de-identify the information. However, Schedule 1, Part 2, Section 4.4 of the *Privacy Act* provides that the entity must comply with APPs 5-13.

APP 6 outlines the framework governing the circumstances under which an APP entity can use or disclose personal information. An APP entity can use or disclose personal information if it is relevant to the 'primary purpose' of collecting that information. In 2020, the Australian Information Commissioner sued Facebook (now Meta) for inter alia disclosing the personal and sensitive information of Australian Facebook users for a purpose other than that for which it was collected between 2014 and 2015, thereby contravening APP 6.[56] According to Perram J, 'APP 6 prevents an organisation which has collected information for a particular purpose to use it for another, except in limited circumstances' (*Facebook v AIC*, 2022). As noted by the Court in this case, personal information can still be used and disclosed for a secondary purpose under certain circumstances. These exceptions, contained under Schedule 1 of the *Privacy Act*, include situations where the APP entity is an organisation and a permitted health scenario exists, or when the secondary use or disclosure is mandated by an Australian law or an order of a court or tribunal. This APP is relevant in the context of satellites and natural disasters because any personal information collected via satellite during a natural disaster could be used and disclosed for the primary purpose of collecting data to ensure safety. More importantly, breach of this APP could lead to unauthorised surveillance or uncontrolled data generation and use (Caron et al., 2016: 10). Part VIA of the *Privacy Act* is closely related to the provisions of APP 6 and contains special provisions that apply to emergency situations or disasters (which by necessary implication includes natural disasters). It specifies how personal information obtained during a declared[57] emergency or disaster should be handled by entities that obtain such information. The entities permitted to handle this information are agencies, organisations, and persons (*Privacy Act 1988* (Cth) s. 80P(7)). While agencies can disclose information to other agencies, State or Territory authorities, organisations, entities involved in disaster management, or even a person responsible to an affected individual (*Privacy Act 1988* (Cth) s. 80P(1)(c)), organisations or any other person can only disclose such information to

[56] Byrne, E. (2023, March 7). *High Court to decide if Facebook is liable for the possible breach of 300,000 Australians' personal data.* ABC News. https://www.abc.net.au/news/2023-03-07/facebook-in-australian-high-court-over-data-breach/102061004

[57] The Prime Minister is empowered under Section 80J to make a declaration of emergency.

agencies, entities providing services to affected individuals, and entities prescribed by regulation or the Minister (*Privacy Act 1988* (Cth) s. 80P(1)(d)). This allows for flexibility in expanding the categories of entities that can access personal information of individuals affected by natural disasters as needed. However, the practical applicability of this provision to instances where personal data is collected through remote sensing during natural disasters remains uncertain, especially when entities are operating from outside Australia's territorial borders.

APP 8 allows for cross-border disclosure of data collected and works in conjunction with Section 16C of the *Privacy Act*. APP 8 stipulates that if data is to be disclosed cross-border, the APP entity responsible for the disclosure must take reasonable steps to ensure that the recipient overseas does not violate any of the APP principles (*Privacy Act 1988* (Cth) APP 8.1). The APP entity disclosing the information is accountable for any failure of the overseas entity to comply with the APPs. In the event that an APP entity wishes to disclose data collected from a natural disaster to an overseas entity, it is required to ensure that the recipient adheres to these principles. Breach of this APP could lead to uncontrolled generation and use, and information security risks (Caron et al., 2016).

APP 11 governs the security of personal information collected by an APP entity. Breach of this APP could lead to uncontrolled generation and use, inadequate authentication, and information security risks (Caron et al., 2016). The Court in *Facebook v AIC* (2022) held that Facebook was in breach of APP 11 as it failed to implement measures to obtain consent directly from the affected Australian users before disclosing their personal information. It is mandatory for any APP entity collecting personal information to safeguard it against potential unauthorised use, loss, disclosure, alteration, or access. Additionally, once the personal information is no longer required by the APP entity, it must either be destroyed, or de-identified to prevent identification of the relevant individual (*Privacy Act 1988* (Cth) APP 11.2).

It is important to note that a person's data privacy may potentially be breached when their image is captured by remote sensing technologies when such technologies are used for monitoring purposes (Maniadaki et al., 2021). Privacy breaches may still occur even if the use is for ostensibly beneficial reasons such as search and rescue efforts during natural disasters. Non-disclosure of the purpose for data collection, details of the entity collecting such data, may exacerbate the unease and leave data subjects feeling that their right to control the use of their personal information has been unjustly compromised (Maniadaki et al., 2021). This may be the case where the person has not consented to the use of their image. The issue of consent highlights some limitations for the scope of the *Privacy Act* because if a person consents to their image being held, collected, or used by an APP entity, the *Privacy Act* will not apply. This is because consent has two purposes under the *Privacy Act*.[58] The first is that it acts as an exception when an APP entity collects and uses personal images. The second is that consent authorises the use of personal data. This therefore underscores the importance of having in place a legal framework that addresses privacy concerns of those individuals whose personal data might be included in satellite imagery collected during natural disaster management operations.

### *Indonesia*

Similar to Australia, Indonesia also has a responsibility to ensure that its remote sensing activities do not violate international laws, including the right to privacy. However, there is no specific framework in place for regulating remote sensing activities or for addressing key issues relating to data access and international cooperation (Zunnuraeni et al., 2020). The *Space Law* and

[58] Sch 1, APPs 3.3 (a), 6.1 (a) of the *Privacy Act*.

the *Government Regulation No. 11 of 2018 Concerning Remote Sensing (GR 11/2018)* cover technical aspects of remote sensing, but not regulations for private entities engaged in remote sensing activities (Sitanggang, 2018).

The *Space Law* requires all government remote sensing activities to be conducted by the National Research and Innovation Agency, and only for specific purposes (Sitanggang, 2018). Prior to the passing of the *Personal Data Protection Law (PDP Law)*[59] in 2022, the regulation of private entities with regards to data privacy was not covered by specific laws but was part of Indonesia's broader privacy laws such as *Government Regulation No. 71 of 2019 Regarding Implementation of Electronic Systems and Transactions* and the *Minister of Communication and Informatics Regulation No. 20 of 2016 Regarding Personal Data Protection in Electronic Systems*. It was generally accepted under these earlier regulations that the collection and use of personal data required express consent from the data owner. However, these regulations were not comprehensive and only applied to specific electronic systems, instead of all telecommunication systems.[60]

The *PDP Law* now provides comprehensive rules for processing personal data, which can also apply to personal data collected during remote sensing activities.[61] Article 2 of the *PDP Law* applies to any individual, corporation, public agency, or international organisation that carries out activities within Indonesia, or outside Indonesia that may have legal consequences within Indonesia or affect Indonesian citizens. The *PDP Law* defines personal data as any data concerning a person, whether identified or who may be identified independently or combined with other information, either directly or indirectly, through an electronic or non-electronic system. Data subjects have specific rights set out under Article 5-14 of the *PDP Law*, including the right to be informed about the purpose of data collection, how the data will be used, and the liability and obligations of the party requesting the personal data. Data subjects also have the right to withdraw their consent at any time.

As previously noted, prior to the *PDP Law*, consent was the primary basis for processing personal data. While the *PDP Law* maintains this requirement, it also recognises, under Article 20, other grounds for processing personal data, including fulfilling contractual obligations, meeting legal obligations of the controller, protecting the vital interests of the data subject, performing public duties for public interest or service, or exercising lawful authority of the controller, and the processing of personal data to fulfill other lawful interests. Article 65 and 66 of the *PDP Law* prohibits certain uses of personal data, such as illegally obtaining or collecting personal data, unlawfully disclosing personal data, using personal data of another in a manner that contravenes the law, and creating false or fake personal data that may cause harm to other persons. Infractions of the *PDP Law* carry varying sanctions, ranging from fines to imprisonment. The law has a transitional period of two years for compliance from the date of its enactment, and a data protection authority will be established pursuant to Article 58 through a presidential regulation, reporting directly to the president.

---

59 Law No. 27 of 2022 on Protection of Personal Data.

60 Iskandar, E., Lubis, D.B., & Hartanto, A.W. (2023, January 6). *The technology, media and telecommunications review: Indonesia.* The Law Reviews. https://thelawreviews.co.uk/title/the-technology-media-and-telecommunications-review/indonesia

61 Panggabean, K., Purba, J., & Karina, T. (2022, October). *Highlights of Indonesia's personal data protection law.* Norton Rose Fulbright. https://www.nortonrosefulbright.com/en/knowledge/publications/31bce8f0/highlights-of-indonesias-personal-data-protection-law

## Liability for misuse of satellites

### Liability and responsibility under international legal framework

As previously discussed, the main international frameworks regarding use of satellites for remote sensing and disaster management are not legally binding, and do not deal with data privacy concerns arising from misuse of satellites. Thus, liability for misuse of satellites which results in privacy breaches might be difficult to impose if reliance is placed solely on the *Remote Sensing Principles* and *Disaster Charter*. Also, it is debatable whether the *Liability Convention*,[62] which deals with liability arising from damages caused by space objects, would cover violations of individual privacy rights (Nafis et al., 2021). Based on Articles II and III of the Convention, it has been argued that the Convention was primarily designed to address physical damages[63] collisions between spacecrafts and component parts (Christol, 1980; Dodge, 2014).

Notwithstanding, liability can arise under general international law if a State can successfully argue that another State's activities, including those of its private actors or corporations, caused damage to it or its nationals (Schmalenbach, 2022).[64] For instance, State A could argue that State B's remote sensing activities violated the privacy of State A's nationals. In addition, most of the principles under the *Remote Sensing Principles* restate the rules under the *Outer Space Treaty* or allude to general principles of international law.[65]

Also, the Preamble of the *Disaster Charter* refer to the *Remote Sensing Principles* which implies that the Principles should be observed when carrying out remote sensing activities under the *Disaster Charter*. Article VI of the *Outer Space Treaty* provides that 'State Parties to the Treaty shall bear international responsibility for national activities in outer space... whether such activities are carried on by government agencies or by non-government entities...' This means that States are responsible for any wrongdoing caused in outer space either by the government, or by private entities. This would extend to commercial activities. Remote sensing is listed as a type of commercial activity which is increasingly being carried out by private entities (Gupta & Raju, 2019).

Resultantly, through a combined reading of the above international instruments, States can be held responsible for remote sensing activities carried out by them, and their private entities during natural disasters.[66] Since Australia and Indonesia are parties to the *Outer Space Treaty*, it would therefore be important to examine the liability provisions under their various national laws as they relate to satellites.

### Liability and responsibility under national legal framework

#### *Australia*

The *Space Act* sets out legal liability for any damage caused in outer space by a space object launched by Australia. Section 8 of the Act defines 'damage' in the same way as the *Liability*

[62] Convention on International Liability for Damage Caused by Space Objects (UN GA Res 2777 (XXVI), annex)—adopted on 29 November 1971, opened for signature on 29 March 1972, entered into force on 1 September 1972.

[63] Article I define damage as 'loss of life, personal injury or other impairment of health; or loss of or damage to property of States or of persons, natural or juridical, or property of international intergovernmental organizations.

[64] A common example of this is environmental pollution. Here, States have claimed that transboundary pollution injures their rights to enjoy their territory or that the transboundary pollution is causing injury to their nationals.

[65] *See* Principle IV, *Remote Sensing Principles.*

[66] *See* Principle XIV of the *Remote Sensing Principles* which buttresses this point.

*Convention*. Therefore, the same argument made earlier applies here, which is that violation of privacy rights resulting from the misuse of satellites for remote sensing activities are not covered by this Act. Notwithstanding that the *Space Act* liability provisions might only apply to physical damage involving satellites during launch into outer space or re-entry into Earth, the *Privacy Act* will apply to privacy breaches relating to data collected through satellites or other means.

By virtue of Section 13(1)(a) of *Privacy Act,* an act or practice that breaches any of the APPs in relation to personal information about an individual is an interference with the privacy of such an individual. Where this act or practice is done repeatedly by the APP entity, such would be a serious and repeated interference with privacy and is classified as a civil liability under Section 13G. Under Section 13G (2) and (3), the maximum penalty that can be imposed on a body corporate for this contravention is $50,000,000, and $2,500,000 for a person other than a body corporate. It should be noted that by virtue of Section 80U, only the Information Commissioner is authorised to bring an application before the Federal Court or Federal Circuit Court and Family Court of Australia in respect of a civil liability action.[67] Thus, if a satellite is used by an APP entity for remote sensing activities that violate the provisions of any of the APPs under the *Privacy Act*, the following enforcement actions can be taken against that entity — civil liability actions, infringement notices, enforcement undertakings, and injunctions.

### *Indonesia*

Pursuant to Article 41(1) of the *Space Law,* Indonesia is responsible for overseeing all of its national space activities and is accountable for any wrongful acts that result from the misuse of satellites. Like Australia, Indonesia has provisions in its *Space Law*[68] that deal with liability for damage caused in space, on Earth or to an aircraft in flight. However, damage in this context is limited to physical damage and does not cover liability for privacy breaches resulting from misuse of satellites.

Regarding the violation of personal data under the *PDP Law*, both administrative and criminal sanctions may be imposed. In the absence of a standalone regulatory framework specific to the misuse of satellites in the context of privacy breaches, the provisions of the *PDP Law* will be applicable. As provided under Article 67 and 68 of the *PDP Law*, criminal sanctions include a fine of up to IDR 6 billion and/or imprisonment of up to six (6) years. Administrative sanctions include written warning, temporary suspension of personal data processing activity, deletion of personal data, or imposition of administrative fines under Article 57. These penalties may be imposed on the management, controller, instructor, beneficial owner, or corporation.

## Conclusion

In conclusion, it is apparent that international rules on the use of satellites for remote sensing activities generally lack binding force, and they do not effectively address the issue of privacy breaches that may result from satellite misuse. International human rights framework such as UDHR and ICCPR which provide for right to privacy are broad, and their provisions are not sufficiently robust to cover use of satellite data, especially for commercial or private use. In the context of natural disasters, it is even more important to ensure data privacy concerns are given due consideration

[67] *See also* Flannery, A., & Cass, S. (2020, May 21). Australia: Liability for breaches of Privacy Act to increase, but class actions unlikely to be supported. *Mondaq*. https://www.mondaq.com/australia/data-protection/938568/liability-for-breaches-of-privacy-act-to-increase-but-class-actions-unlikely-to-be-supported

[68] *See* Article 76(2).

while the satellites are being used for remote sensing during the disaster management process (Mosteshar, 2016).

As already stated, with advancements in technology, it becomes even more probable that data collected during natural disasters by the sophisticated sensors placed on LEO satellites would include those capable of identifying individuals. As a result, safeguards need to be in place to ensure that satellites continue to play the important role of aiding in rescue efforts during natural disasters without infringing on individuals' privacy rights in the process. As this article highlighted, it is a challenging feat to try to balance the public interest in disaster management with individual privacy rights, mainly because the expectation of privacy during natural disasters differs considerably from non-emergency situations (Sanfilippo et al., 2020). However, this should not be a basis for countries to take with levity the need to adequately consider and take steps to mitigate the materialisation of the risks of privacy breaches resulting from remote sensing activities during natural disasters.

In the absence of a uniform set of rules at the international level that adequately regulates data sharing or privacy issues, individual countries can address these issues through the instrumentality of their national laws.[69] In the case of Australia and Indonesia, both countries lack standalone legal frameworks that specifically address privacy breaches caused by misuse of satellites during natural disasters. However, a combination of space activity legislation and data protection laws in both countries can serve as a temporary measure to determine liability for privacy breaches resulting from satellite misuse during natural disasters.

Ultimately, it is recommended that both countries review their existing legal frameworks to address the potential unintended consequences of advancing remote sensing capabilities on data privacy. Since both countries have provisions in their space legislation[70] requiring adequate insurance in respect of liability for damage (Kerkonian, 2021), the scope of what constitutes liability for damage under both legal frameworks could be expanded to explicitly include provisions relating to privacy.

Another suggestion is for both countries to make remote sensing activities subject to licensing through their domestic laws. This is supported by the provision of Article VI of the *Outer Space Treaty* which imposes an obligation on countries to authorise and supervise space activities within their respective jurisdictions. This authorisation regime, which could be in form of compulsory licensing for entities engaged in remote sensing activities, provides an opportunity for both countries to impose restrictions or conditions on space activities, including provisions for respecting privacy. These restrictions could include satellite capacity limits, resolution limits for satellite images, exclusive acquisition of rights to relevant satellite images[71], requirements of blurring personal identifying information in satellite images, and more. National legislation should play a significant role in addressing privacy concerns arising from remote sensing activities conducted with LEO satellites (Linden, 2016), as not only States, but also private entities and individuals globally are increasingly involved in commercial remote sensing activities. Expressly including respect for privacy as a condition for engaging in space activities would be a pioneering move and set a precedent for other countries to follow.

---

69 Rotola, G., Farrar, L., Nasr, F., Wiser, L., Navalgund, R., Ciarravano, L., & Grattan, K. (2022, January). *Earth Observation Data, Climate Change, and Human Rights*. Jus Ad Astra. http://www.jusadastra.org/SGAC-Law-Climate-Change.html

70 Space (Launches and Returns) Act, 2018, Section 48; Law No 21 of 2013 Concerning Space Activities, Article 84(1).

71 Rotola, G., Farrar, L., Nasr, F., Wiser, L., Navalgund, R., Ciarravano, L., & Grattan, K. (2022, January). *Earth Observation Data, Climate Change, and Human Rights*. Jus Ad Astra. http://www.jusadastra.org/SGAC-Law-Climate-Change.html

## References

1. Alazab, M., Hong, S.-H., & Ng, J. (2021). Louder bark with no bite: Privacy protection through the regulation of mandatory data breach notification in Australia. *Future Generation Computer Systems*, *116*, 22–29. https://doi.org/10.1016/j.future.2020.10.017
2. Boon, H. (2013). Preparedness and vulnerability: An issue of equity in Australian disaster situations. *Australian Journal of Emergency Management*, *28*(3), 12–16. https://search.informit.org/doi/10.3316/agispt.20132324
3. Caron, X., Bosua, R., Maynard, S. B., & Ahmad, A. (2016). The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. *Computer Law & Security Review*, *32*(1), 4–15. https://doi.org/10.1016/j.clsr.2015.12.001
4. Christol, C. Q. (1980). International liability for damage caused by space objects. *American Journal of International Law*, *74*(2), 346–371. https://doi.org/10.2307/2201505
5. Coffer, M. M. (2020). Balancing privacy rights and the production of high-quality satellite imagery. *Environment Science & Technology*, *54*(11), 6453. https://doi.org/10.1021/acs.est.0c02365
6. Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view. *Computer Law & Security Review*, *34*(3), 477–495. https://doi.org/10.1016/j.clsr.2018.01.005
7. De Beer, A. (2020). The refusal of access to high-resolution remote sensing data for reasons of national security–a rule of customary international law? *Tydskrif Vir Die Suid-Afrikaanse Reg* [*Journal of South African Law*], *2020*(1), 74–87.
8. Dodge, M. (2014). Earth Observation and the Needs of the Many: The Future Structure of International Disaster Relief Law and Management. *Annals of Air and Space Law*, *39*, 355.
9. Sitanggang, D.F.D. (2018). International Law Analysis of the Restrictions Imposed on Remote Sensing Satellite Through Shutter Control. *Jurnal Mimbar Hukum*, *30*(2), 389–406. https://doi.org/10.22146/jmh.31151
10. Emery, W., & Camps, A. (2017). *Introduction to satellite remote sensing: Atmosphere, ocean, land and cryosphere applications*. Elsevier. https://doi.org/10.1016/C2015-0-04517-8
11. Freeland, S., & Ireland-Piper, D. (2022). Space law, human rights and corporate accountability. *UCLA Journal of International Law and Foreign Affairs, 26* (1), 1–34.
12. Freeland, S., & Pecujlic, A. N. (2018). How do you like your regulation: Hard or soft? : The Antarctic Treaty and the Outer Space Treaty compared. *National Law School of India Review, 30*(1), 11–36. https://repository.nls.ac.in/nlsir/vol30/iss1/2
13. Froehlich, A., & Seffinga, V. (2018). *National space legislation: A Comparative and Evaluative Analysis*. Springer. https://doi.org/10.1007/978-3-319-70431-9
14. Georgiades, E. (2020). A Right that should've been: Protection of personal images on the Internet. *IDEA: The Law Review of the Franklin Pierce Center for Intellectual Property*, *61*(2), 275–327.
15. Gummadi, G., & Gupta, B. (2022). Remote sensing data and international IP laws. *Journal of Legal Subjects*, *20*(2), 13–28. https://doi.org/10.55529/jls22.13.28
16. Gupta, B., & Raju, K. (2019). Understanding international space law and the liability mechanism for commercial outer space activities—unravelling the sources. *India Quarterly*, *75*(4), 555–578. https://doi.org/10.1177/0974928419874553
17. Hakim, W. L., & Lee, C.-W. (2020). A review on remote sensing and GIS applications to monitor natural disasters in Indonesia. *Korean Journal of Remote Sensing*, *36*(6_1), 1303–1322. https://doi.org/10.7780/kjrs.2020.36.6.1.3
18. Housen-Couriel, D. (2016). Cybersecurity threats to satellite communications: Towards a typology of state actor responses. *Acta Astronautica*, *128*, 409–415. https://doi.org/10.1016/j.actaastro.2016.07.041

19. Kuner, C., & Marelli, M. (2020). *Handbook on data protection in humanitarian action*. The International Committee of the Red Cross. https://shop.icrc.org/download/ebook?sku=4305.01/002-ebook
20. Ito, A. (2011). *Legal aspects of satellite remote sensing*. Brill.
21. Mosteshar, S. (2016). Regulation of remote sensing by satellites. In R. Jakhu, & P.S. Dempsey (Eds.), *Routledge Handbook of Space Law* (pp. 144-159). Routledge. https://doi.org/10.4324/9781315750965
22. National Research Council. (1996). *Cryptography's role in securing the information society.* National Academy Press. https://doi.org/10.17226/5131
23. Nishara, N., & Pandey, R. (2015). Enhancing security in public clouds using data anonymization techniques. *International Journal of Computer Applications*, *128*(1), 33–36. https://doi.org/10.5120/ijca2015906428
24. Kaku, K. (2019). Satellite remote sensing for disaster management support: A holistic and staged approach based on case studies in Sentinel Asia. *International Journal of Disaster Risk Reduction*, *33*, 417–432. https://doi.org/10.1016/j.ijdrr.2018.09.015
25. Kemp, K. (2022). Strengthening enforcement and redress under the Australian Privacy Act. *Global Privacy Law Review*, *3*(3), 150–162. https://doi.org/10.54648/gplr2022016
26. Kerkonian, A. D. (2021). National regulation of space activities. In A.D. Kerkonian (Ed.), *Space Regulation in Canada: Past, Present and Potential* (pp. 235–319). Springer. https://doi.org/10.1007/978-3-030-68692-5
27. Linden, D. (2016). The impact of national space legislation on private space undertakings: Regulatory competition vs. harmonization. *Journal of Science Policy & Governance*, *8*(1), 1–17.
28. Maniadaki, M., Papathanasopoulos, A., Mitrou, L., & Maria, E.-A. (2021). Reconciling remote sensing technologies with personal data and privacy protection in the European Union: Recent developments in Greek legislation and application perspectives in environmental law. *Laws*, *10*(2), No. 33. https://doi.org/10.3390/laws10020033
29. Nafis, R. W., Supriyadhie, M. K., & Adya, P. (2021). The Utilization of GSO by Indonesia as a Subjacent State Based on Space Treaty 1967. *Proceedings of the 1st International Conference on Science and Technology in Administration and Management Information, ICSTIAMI 2019, 17-18 July 2019, Jakarta, Indonesia*. http://dx.doi.org/10.4108/eai.17-7-2019.2303333
30. Nugraha, T. R., Putro, Y. M., Aditya Nugraha, R., & Christiawan, R. (2022). Indonesian space activities: The long and winding road. *Astropolitics*, *20*(2–3), 238–250. https://doi.org/10.1080/14777622.2022.2141113
31. Page, J., & Besco, L. (2021). Dispossession through collision: Low-Earth orbit and planetary sustainability. *Territory, Politics, Governance*, 1–18. https://doi.org/10.1080/21622671.2021.1903543
32. Qu, Y., Nosouhi, M. R., Cui, L., & Yu, S. (2019). Privacy preservation in smart cities. In D. B. Rawat, & K. Z. Ghafoor. *Smart cities cybersecurity and privacy* (pp. 75–88). Elsevier. https://doi.org/10.1016/C2017-0-02545-4
33. National Research Council. (2001). Realizing the potential of remote sensing. In *Transforming remote sensing data into information and applications*. National Academies Press. https://doi.org/10.17226/10257
34. Sanfilippo, M. R., Shvartzshnaider, Y., Reyes, I., Nissenbaum, H., & Egelman, S. (2020). Disaster privacy/privacy disaster. *Journal of the Association for Information Science and Technology, 71*(9), 1002–1014. https://doi.org/10.1002/asi.24353
35. Santos, C., & Rapp, L. (2019). Satellite imagery, very high-resolution and processing-intensive image analysis: Potential risks under the GDPR. *Air and Space Law, 44*(3), 275–295. https://doi.org/10.54648/aila2019018
36. Sheinidashtegol, P., Musaev, A., & Atkison, T. (2019). Investigating personally identifiable information posted on Twitter before and after disasters. In Y. Xia, L.-J. Zhang. *Services — SERVICES 2019: 15th World Congress, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings* (pp. 31–45). Springer. https://doi.org/10.1007/978-3-030-23381-5_3

37. Sainty, K., & Rowe, B. (2020). OAIC v Facebook. *Communications Law Bulletin*, *39(2)*. http://www5.austlii.edu.au/au/journals/CommsLawB/2020/19.pdf
38. Sastrawidjaja, L., & Suryanegara, M. (2018). Regulation challenges of 5G spectrum deployment at 3.5 GHz: The framework for Indonesia. *Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS)*, 213–217. http://dx.doi.org/10.1109/EECCIS.2018.8692880
39. Schmalenbach, K. (2022). Convention on International Liability for Damage Caused by Space Objects. In P. Gailhofer, D. Krebs, A. Proelss, K. Schmalenbach, R. Verheyen (Eds.), *Corporate liability for transboundary environmental harm: An international and transnational perspective* (pp. 523–536). Springer Cham. http://dx.doi.org/10.1007/978-3-031-13264-3_11
40. Singh, R., Kaul, S., & Deva Rao, S. (2012). *Current developments in air space law*. National Law University Press.
41. Supancana, I. B. R. (2006). *Space law development in retro and prospect*. Mitra Karya Publisher.
42. Supancana, I. B. R. (2015). How the progressive development of outer space law affects the formulation of national space legislation: The experience of Indonesia. *Air and Space Law*, *40*(1), 93–106. https://doi.org/10.54648/aila2015009
43. Svantesson, D. J. B. (2014). The extraterritoriality of EU data privacy law-its theoretical justification and its practical effect on US businesses. *Stanford Journal of International Law*, *50*(1), 53–102.
44. Svantesson, D. J. B. (2015). Extraterritoriality and targeting in EU data privacy law: The weak spot undermining the regulation. *International Data Privacy Law*, *5*(4), 226–234. http://dx.doi.org/10.1093/idpl/ipv024
45. Tatem, A. J., Goetz, S. J., & Hay, S. I. (2008). Fifty years of Earth-observation satellites: Views from space have led to countless advances on the ground in both scientific knowledge and daily life. *American Scientist*, *96*(5), 390–398.
46. Tronchetti, F. (2015). Legal aspects of satellite remote sensing. In F.G. von der Dunk, & F. Tronchetti (Eds.), *Handbook of Space Law* (pp. 501–553). Edward Elgar Publishing.
47. Verco, E. (2021). Satellites are cyber insecure: We need regulation to avoid a disaster. *Australian National University Journal of Law and Technology*, *2*(2), 57–94. https://anujolt.org/article/30203-satellites-are-cyber-insecure-we-need-regulation-to-avoid-a-disaster
48. von der Dunk, F. (2013). Outer space law principles and privacy. In R. Purdy, & D. Leung (Eds.), *Evidence from Earth observation satellites* (pp. 241–258). Brill Nijhoff. https://doi.org/10.1163/9789004234031
49. von der Dunk, F. (2002). United Nations principles on remote sensing and the user. In R. Harris (Ed.), *Earth observation data policy and Europe* (pp. 29–40). CRC Press.
50. von Dietze, A., & Allgrove, A.-M. (2014). Australian privacy reforms—An overhauled data protection regime for Australia. *International Data Privacy Law*, *4*(4), 326–341. http://dx.doi.org/10.1093/idpl/ipu016
51. Yu, M., Yang, C., & Li, Y. (2018). Big data in natural disaster management: A review. *Geosciences, 8*(5), No. 165. https://doi.org/10.3390/geosciences8050165
52. Zollner, K. (2018). United Nations platform for space-based information for disaster management and emergency response (UN-SPIDER). In C. Brünner, G. Königsberger, & A. Rinner (Eds.), *Satellite-based Earth observation.* Springer. 235–241. https://doi.org/10.1007/978-3-319-74805-4_24
53. Zunnuraeni, Z., Minollah, M., Ilwan, M., & Nurbani, E. S. (2020). Legal concept for remote sensing as the foundation of Indonesian space law. Proceedings of the 1st Annual Conference on Education and Social Sciences (ACCESS 2019). Atlantis Press. 83–85. https://doi.org/10.2991/assehr.k.200827.022

Information about the authors:

**Temitope Lawal*** — Ph.D. Candidate, Faculty of Law, Bond University, Robina, Queensland, Australia.
tlawal@bond.edu.au
ORCID: https://orcid.org/0000-0002-3844-3945

**Melanie Jackson** — Senior Teaching Fellow, Faculty of Law, Bond University, Robina, Queensland, Australia.
mjackson@bond.edu.au
ORCID: https://orcid.org/0000-0002-5386-4406

**Eugenia Georgiades** — Ph.D. in Law, Assistant Professor, Faculty of Law, Bond University, Robina, Queensland, Australia.
egeorgia@bond.edu.au
ORCID: https://orcid.org/0000-0002-4040-7652

Сведения об авторах:

**Лаваль Т.*** — аспирант, юридический факультет, Университет Бонд, Робина, Квинсленд, Австралия.
tlawal@bond.edu.au
ORCID: https://orcid.org/0000-0002-3844-3945

**Джексон М.** — старший преподаватель, юридический факультет, Университет Бонд, Робина, Квинсленд, Австралия.
mjackson@bond.edu.au
ORCID: https://orcid.org/0000-0002-5386-4406

**Георгиадес Е.** — Ph.D. in Law, доцент, юридический факультет, Университет Бонд, Робина, Квинсленд, Австралия.
egeorgia@bond.edu.au
ORCID: https://orcid.org/0000-0002-4040-7652