LmunA 2022

Research report

Forum:	UNCOPUOS
Issue:	The potential legal implications of breaches of privacy in relation to satellites in global space exploration
Student Officer:	Pieter van Lelyveld & Ayumie Pathirana
Position:	Main Chair & Deputy Chair

LMUNA
Lorentz Lyceum
Model United Nations
Arnhem

Table of Contents

LmunA 2022

Introduction

With the rise of space exploration came the rise of satellites in outer space and aerospace experts predict that in 2022 the Earth will have over 5,000 operational orbiting satellites. This extreme network of continuous ground-to-space connections has a long list of advantages and is the core of our modern society. For example, this satellite network makes global communication affordable and easy. It is also used for geographical data collection, analysis and global sharing. This relatively new sector of space-to-ground information sharing leads to a global interest in data corruption.

Figure 1. An image of WorldView-3, the most powerful image satellite ever, 2022

We are left with the task of creating a network of 5,000 international communication, TV and data satellites in order to form a strong network of communication sharing without the risk of data breaches, or “hacks”, jeopardising global information sharing. With that quest, humankind is also stuck with other issues. One of the bigger issues in outer space satellite networks is the privacy regulations and the vulnerability of mobile users’ data. Someone’s geolocation can be tracked, mobile data can be corrupted, IP addresses were stolen and even data sets like fingerprints can be found. International laws do obviously apply in this issue, however, the laws concerning international privacy protection are often not truly international and do not apply to all SpaceTech. Legislative networks such as the General Data Protection Regulations (GDPR), the Protection of Personal Information Act (POPIA) or the California Consumer Privacy Act (CCPA) take action toward data protection in general, however, they leave a grey area in outer space. In this research report, all aspects of privacy protection in outer space concerning satellites will be assessed.

Definitions of key terms

World Wide Web

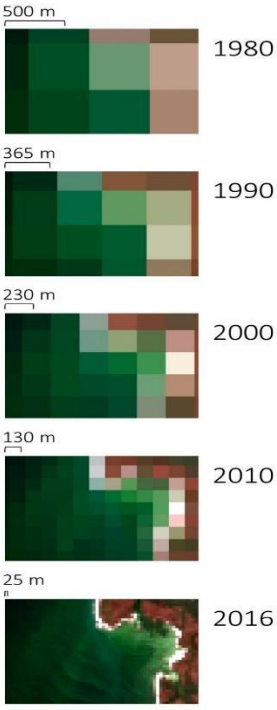
A platform for online information sharing through the Internet. This allows for people to share and access information from all over the world and communicate globally.

Hacking

The act of using technology to gain unauthorised access to information in a system belonging to an individual, organisation or nation.

Space Cloud Computing

Companies instantly provide different services such as data storage, software or networking to a user. These Cloud Computing centres are often located on Earth but recently some multinationals have started developing these Clouds in outer space.



Virus
A series of code that has the ability to replicate itself and at the same time digitally attack another device, server or cloud. Viruses often have the aim to disrupt or destroy systems or even entire companies.

Outer space
The vacuous region that exists beyond the atmosphere of the earth. It is important to note that outer space does not begin at a precise altitude from the Earth's surface. However, international frameworks uphold the Kármán line as a starting point located 100 km (62 mi) above sea level.

The International Right to Privacy
Defined by the Universal Declaration of Human Rights (UDHR): "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, or correspondence, or to unlawful attacks on his honour and reputation."

Malware
Computer software or programs designed to impair or even destroy computers.

Digital Age
The Digital Age is an era of human history based on information computerization. The Digital Age is associated with the Digital Revolution, which refers to the growing number of people connected online in the world.

Firewall
A protection system for computers to prevent unauthorised access by for example hackers.

Cyber Security
Cyber Security is the practice of protecting mobile instruments such as servers, computers or even satellite systems from external threats.

General overview

Satellites serve many purposes, including observation and imagery of the planet Earth, navigational information, and enabling communication services. In 1957, the first satellite to ever enter orbit, Sputnik 1, was launched, making Russia the first space power and winning the first stage of the space race. With Sputnik 1 came an incentive for other countries to follow suit, not wanting to get behind, and within months, many other countries had attempted to launch their own satellites. Sputnik 1's goal was to place a radio transmitter into space, which it successfully accomplished. However, Sputnik 1 did not have much use other than to transmit radio signals down to Earth. Although its significance was grand, satellites had a long way to go until they reached the level of sophistication current satellites have.

In 1959, the first successful launch of a satellite equipped with a camera occurred, and nearly a month after the initial launch, the first orbital photographs of Earth were made. Although this brought with it near-boundless opportunities, the public was already beginning to

worry about breaches of privacy that satellites could bring. Of course, it was later proven that, with the level of technology available at the time, they would likely not be able to see close enough to spy on the general public. This seems to have assuaged the fears related to satellites, but not for long, before more potential for privacy breaches appeared. Satellite imagery continued to improve over the years, pixel sizes improving almost 20-fold, reaching a shocking 25m in 2016 (see fig.2). Navigational systems continue to improve alongside camera quality, creating a potential issue in the

With the launch of Telstar 1, a satellite launched by an American telecommunications company, the first satellite phone call was made. This opened up many possibilities that were incomprehensible before, in the age of short-range cellular calls. Within years, satellite phones had become all the rage, and yet, just as with the satellite camera, fears began to pervade the public's perception of the technological marvel. Although relatively difficult, satellite calls can be tracked and eavesdropped upon, posing a potential threat to personal privacy. With the advent of satellite internet access, satellites were given the ability to observe almost every aspect of a person's digital life, and now, in the 21st century, satellites have improved at a remarkable rate, with high-resolution cameras and an innumerable number of calls occurring over satellites every day. This has reintroduced many fears related to privacy breaches in terms of satellite data.

Figure 2. Depiction of improvement in satellite imagery, Environmental Science and Technology Journal, 2018

At the moment, satellite data collection is a serious issue, and although it has been dealt with in different ways in different countries, the fear of someone's Big Brother-Esque control over the data and digital life of huge amounts of people is still very much prevalent today. According to Article 12 of the UDHR, 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.' In theory, this would prove to be a safeguard against any potential breaches of privacy, yet there have been instances in which this has occurred. In 2021, in the United States alone, there were an estimated 1.8 billion data breaches, affecting nearly 300 million individuals in that year. Since 2005, the amount of data breaches has risen by 1 billion, affecting countless lives. Data breaches have resulted in many lawsuits, claiming breach of privacy and contract (in cases in which a conglomerate may sue a satellite holdings company). Such lawsuits have become more and more common, each affecting millions of people (see timeline section). Many member states have attempted to fix this issue, by setting limitations on what satellites can access, or on how high-quality their images and data can be. However, this has not proven very useful, as in the age of digital lives, many of such regulations have been lifted, further encouraging such data breaches and the lawsuits that nearly inevitably follow.

Major parties involved

The United States of America

The U.S. is the leading facilitator for imaging and communication satellites. The U.S. are also the home of the National Aeronautic Space Administration (NASA) and SpaceX: two of the leading space organisations globally. Now the United States Government has been rapidly developing new governmental bodies in order to create enough technology to keep up with its 'competitors'. Most memorable would be the sixth military branch created by President Donald Trump back in 2019, the United States Space Force. This new military branch has the main aims of space security, space combat, information mobility and space domain awareness. The Biden administration was relatively laid back on space security to the point of doubting the sixth army division. Nonetheless the Biden administration has increased their cybersecurity after numerous threats surrounding the Ukraine conflict. U.S. President Biden stated this March: "*This is a critical moment to accelerate our work to improve domestic cybersecurity and bolster our national resilience. I have previously warned about the potential that Russia could conduct malicious cyber activity against the United States, including as a response to the unprecedented economic costs we've imposed on Russia alongside our allies and partners.*"

The Russian Federation

The Russian Federation used to be the superior force in outer space. Nowadays Russia has lost that position but the Russian government, most notably the Russian state cooperation Roscosmos responsible for all outer space missions, has been enhancing its space program. The current Russian space budget sits at 210 billion Rubles ($2.9 billion), a slight cut from previous years due to Russia's involvement in the Ukrainian war. Russia still heavily relies on their communication and information satellites, and they have always used their satellites to spy on other nations. The Russian fed. is also known for being the nation of hacking. Some more notorious hacks were the NotPetya, BlackEnergy and Colonial Pipeline hacks. This August the Russian fed. also allegedly launched the spy satellite Kosmos 2558 orbiting the same path as military satellite USA 326, U.S. National Reconnaissance Office (NRO) reported.

Figure 3. President J. Biden addressing privacy security in March, 2022

SpaceX

The most notable NGO in space would be SpaceX, with a net worth of 125 billion dollars and a reputation for creating the newest tech the space exploration sector has seen. SpaceX is known for its many cutting-edge projects like the partially reusable Falcon Heavy (known as the most powerful rocket ever) and the Starlink project aiming to create a global internet connection using 30,000 SpaceX satellites, Starlink is the biggest satellite system in the world. Another key project of SpaceX is the still developing Starship, a completely reusable rocket with the ability to fly to Mars. Since its start in 2002 SpaceX has been a major player in space tech development by creating all their rockets in the U.S. and creating the lowest launch cost there is. SpaceX also facilitated some Starlink satellites to Ukraine following governmental orders. These satellites would form a non-Russian communication network for the Ukrainian public. After several hours the Starlink satellites got jammed by a still unknown external party, expert analysts suggest the Russian fed., but after several hours a system update overwrote the signal.

European Space Association (ESA)

The European Space Association (ESA) is a large collective for European nations in order to partake in space exploration. With the combined knowledge and funds from the 22 members, the ESA can achieve striking results far beyond what any European nation could perform standing alone. The ESA mainly focuses on researching celestial bodies and astronomical phenomena as well as the development of satellites and other outer space technology systems. In these proceedings, the ESA works closely with other international space organisations such as JAXA, NASA and Roscosmos. The ESA also serves as the floor for the discussion on International Space Law such as the GDPR. The following European states are members of the ESA: Austria, Denmark, Estonia, France, Germany, Hungary, Ireland, Italy, Luxembourg, Belgium, the Netherlands, Norway, Finland, Poland, Switzerland, Portugal, Romania, Spain, Sweden, Greece, the United Kingdom and lastly the Czech Republic.

Kenya

Kenya's relatively new space program can also be considered as a major party in the privacy security sector, especially in the African Union. With a philosophy opposite to other African space agencies, Kenya Space Agency (KSA) takes the attention of the international community. With new projects like MIDST and club space, they're revolutionising the sector. Although the global media doesn't mention the KSA that much, they are an elite association.

Figure 4. The Executive Board of the KSA March, 2022

Timeline of Key Events

October 8th 1957	Sputnik 1, the first satellite to enter orbit, is launched, thus beginning the space age.
December 13th 1958	The United Nations Office on Outer Space Affairs (UNOOSA) is created by the General Assembly in resolution 'Question of the peaceful use of outer space'.
August 14th 1959	The United States of America's Explorer 6 satellite takes the first ever satellite photographs of Earth.
December 12th 1959	The United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) is created by the General Assembly in resolution 'International co-operation in the peaceful uses of outer space'.
April 1st 1960	The world's first weather satellite is launched, the first practical use satellites had posed for the general public.
1980	Spatial resolution of satellite imaging reaches pixel sizes of roughly 500m.
December 3rd 1986	The General Assembly votes the Principles relating to Remote Sensing of the Earth from Outer Space
1989	The first satellite phone was introduced by Motorola, beginning the increasing demand for satellite communications.
September 6th 2003	Eutelsat, an internet provider based in France, successfully launches the first Internet-ready satellite (the e-BIRD) for consumers.
June 17th 2014	The EU enhances commercial access to observational satellites and in states regulations on the highest possible resolution imagery allowed.

September 19th 2019	Intelsat, a multinational service provider sues OneWeb, a satellite communications company for breach of contract and stealing confidential client information, requesting return on their 1 billion USD investment in the company, marking the largest satellite privacy-related lawsuit to date.

Previous attempts to solve the issue

- The creation of the United Nations Office on Outer Space Affairs (UNOOSA) within resolution 'Question of the peaceful use of outer space', adopted by the General Assembly, 1958, **(A/RES/1348)**

- The United Nations creates the Committee on the Peaceful Uses of Outer Space (UNCOPUOS), within resolution 'International co-operation in the peaceful uses of outer space', by the General Assembly, 1959, **(A/RES/1472)**

- 'Human rights and scientific and technological development: respect for the privacy of individuals and the integrity and sovereignty of nations in the light of advances in recording, and other techniques', report by the Secretary-General, containing potential solutions for issues arising from advancing observational technology, 1973, **(E/CN.4/1116)**

- 'Principles relating to Remote Sensing of the Earth from Outer Space', resolution adopted by the General Assembly, incorporating regulations for satellites collecting data of individuals on Earth, 1986, **(A/RES/41/65)**

- 'The right to privacy in the digital age, resolution adopted by the General Assembly, including mentions of surveillance and sensitive data, 2018, **(A/RES/73/179)**

Possible solutions

The good news is that companies and governments across the board are beginning to take a forward-thinking stance at emerging cybersecurity threats to space equipment, software and communication satellites. Space equipment manufacturers Boeing and Northrop Grumman even hosted a recent webinar discussing the design of space-bound equipment in light of outer space privacy regulations. However, the real power is laying in the hands of the bigger nations and their eagerness to create an internationally binding legal framework.

These two multinationals mainly focused on two points: We need upfront cybersecurity accountability from the very beginning. This doesn't just go for equipment and hardware, but for operating systems and software that shuttles, rockets and satellites will be used. It's easy for engineers or globally distributed software developers to take a product- and functionality-first approach, but emphasising security at all phases of the process is paramount.

Finally, the private and public sectors need to collaborate and conduct as many real-world privacy breach scenarios and exercises before the equipment gets sent into orbit. Things like penetration testing and breach response need to be drilled exhaustively. Because once the equipment is sent into space, it becomes extremely difficult to adjust on the fly if gaps crop up.

The National Institute of Standards and Technology (NIST) in the United States could also play a pivotal role in pushing standardised cybersecurity frameworks. Just last month, NIST introduced a reference document for how privacy standards may be introduced for international space exploration missions. Once NIST receives industry feedback, more concrete recommendations should emerge.

Another issue is individuals placing their personal data on online databases with no thought of who could see and use this content. Therefore, public awareness must be spread to allow the public to see the dangers of spreading confidential information and how they can possibly prevent this. As previously mentioned, UK citizens have already begun using methods such as changing privacy settings, reading privacy policies and deleting cookies.

Looking at the legal scope of the issue, we can see that nations and powerful private organisations need to collaborate and draft a version of an international law framework aiming at alienating privacy breaches in outer space. If the international community accepts these terms the framework should also overlook the responsibility aspect of the issue giving the power to condone certain deeds and redirect claims to intercontinental courts such as the International Court of Justice (ICJ) or even the International Criminal Court (ICC).

With the private sector making even more daring endeavours into orbit, it's undeniable that more of our terrestrial-based economy will be intertwined with space technology and activity. The challenge of safeguarding that infrastructure from hackers is unparalleled, but not impossible. By building on existing private-public partnerships and formulating innovative frameworks that all organisations can adopt globally, we can securely explore the final frontier free from cybercrime and privacy invasion.

Further reading

To fully comprehend the issue, it's important to look at these research links:

I. http://www.un.org/en/ga/69/resolutions.shtml
II. https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/
III. https://www.ohchr.org/en/special-procedures/sr-privacy/international-standards

Bibliography

1. "1958 - Satellite & Spacecraft Launches and Detailed Orbits." *Www.orbitalfocus.uk*, May 2012, www.orbitalfocus.uk/Diaries/Launches/Launches.php?year=1958.

2. Fitchard, Kevin. "With New Satellite Tech, Rural Dwellers Get Access to True Broadband." *Old.gigaom.com*, 1 Oct. 2011, gigaom.com/2012/10/01/with-new-satellite-tech-rural-dwellers-get-access-to-true-broadband/.

3. May, Sandra. "What Is a Satellite?" *NASA*, 12 Feb. 2014, www.nasa.gov/audience/forstudents/5-8/features/nasa-knows/what-is-a-satellite-58.html.

4. Mckenna, Anne, et al. *The Role of Satellites and Smart Devices: Data Surprises and Security, Privacy, and Regulatory Challenges*. 22 June 2019.

5. Mohanta, Nibedita. "How Many Satellites Are Orbiting the Earth in 2021?" *Geospatial World*, 28 May 2021, www.geospatialworld.net/blogs/how-many-satellites-are-orbiting-the-earth-in-2021/.

6. NASA. "Sputnik 1." *NASA*, 4 Oct. 2011, www.nasa.gov/multimedia/imagegallery/image_feature_924.html.
7. Sandwell, David. "Voyager: How Have Satellites Improved in the Last 50 Years?" *Scripps Institution of Oceanography*, scripps.ucsd.edu/news/voyager-how-have-satellites-improved-last-50-years.

8. "Satellite Communication - Development of Satellite Communication." *Encyclopædia Britannica*, 2019, www.britannica.com/technology/satellite-communication/Development-of-satellite-communication.

9. Shufelt, Sydney. "Remote-Sensing Satellites and Privacy: Why Current Regulations Will Ultimately Fail – American University Business Law Review." *Aublr.org*, Mar. 2020, aublr.org/2020/03/remote-sensing-satellites-and-privacy-why-current-regulations-will-ultimately-fail/.

10. “Sputnik 1 Satellite Facts & Launch.” *Study.com*, 2022, study.com/academy/lesson/sputnik-1-satellite-definition-facts-launch.html.

11. Swayne, Matt, and Liam Jackson. “Researchers Detail Privacy-Related Legal, Ethical Challenges with Satellite Data | Penn State University.” *Www.psu.edu*, 10 July 2019, www.psu.edu/news/research/story/researchers-detail-privacy-related-legal-ethical-challenges-satellite-data/.

12. The Guardian. “Data Company Sued by US Government amid Fears of Sensitive Location Tracking.” *The Guardian*, 29 Aug. 2022, www.theguardian.com/technology/2022/aug/29/ftc-sues-kochava-tracking-privacy-data.

13. “Universal Declaration of Human Rights.” *United Nations*, www.un.org/en/about-us/universal-declaration-of-human-rights.

14. Werner, Debra. “Intelsat Sues OneWeb, SoftBank Citing Breach of Contract, Fraud, Conspiracy to Steal Information.” *SpaceNews*, 20 Sept. 2019, spacenews.com/intelsat-sues-oneweb-softbank/.