WHEN OPEN-SOURCE INFORMATION BACKFIRES: SATELLITE IMAGERY AND PRIVACY BREACHES

Matin Pedram,* Siena Chandler,** & Eugenia Georgiades***

ABSTRACT

Open-source intelligence increasingly relies on new technologies to collect, process, and analyze open-source information. The enhancement of satellite imagery capabilities aligns with this goal, providing valuable data from hidden areas that are not easily recognizable. Giving more room to the private sector to invest and innovate in the satellite imaging industry results in remarkable achievements in the size of satellites, the quality of images, pricing, and accessibility of data. High-resolution images and potential live videos of the Earth can foster non-state open-source investigations, resulting in a multiplicity of narratives, where public interest exists. Nonetheless, privacy concerns should not be overshadowed by technological developments. The possible clashes between privacy and satellite imagery might be exacerbated if high-resolution images become widespread and the number of commercial satellite operators multiplies in territories with varying privacy laws. This Article considers privacy laws in Australia, the European Union, and the United States to examine to what extent these legal systems can minimize privacy breaches. It is contended that reasonable expectations of privacy can be an effective test to curb the publication of images infringing on individual privacy.

KEYWORDS: Satellite imagery, Open-source information, commercialization, privacy, reasonable expectation.

TABLE OF CONTENTS

I. INTRODUCTION

In his essay, the director of the Central Intelligence Agency (CIA), William Burns, posits that "in the world of constant technological surveillance," open-source information (OSIF) is part of a chain that unlocks new opportunities for the CIA's analysts.[1] Open-source intelligence (OSINT) is extracted exclusively from "publicly or commercially available information that addresses specific intelligence priorities, requirements, or gaps."[2] Perhaps intelligence services and law enforcement agencies are the main users of this process. Still, more accessible data, like high-resolution images of Earth, prompt amateur analysts, academics, and journalists, all of which are non-state OSINT or non-state open-source investigations, to collect and examine OSIF.[3] Nevertheless, it is not far from reality to claim that criminals may be interested in benefiting from OSINT and targeting their victims in the near future.[4] For example, the lower cost of obtaining commercial

---

This paper was partially 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.

* PhD Candidate, Faculty of Law, Bond University; 14 University Dr, Robina, QLD 4226, Australia; mpedram@bond.edu.au.

** Research Assistant, Faculty of Law, Bond University; siena.chandler@student.bond.edu.au.

*** Associate Professor, School of Law and Justice, University of Southern Queensland; eugenia.georgiades@unisq.edu.au.

Authors would like to thank Shirley Brown for copyediting.

1. William J. Burns, *Spycraft and Statecraft: Transforming the CIA for an Age of Competition*, 103 FOREIGN AFF. 74, 74 (2024).

2. CENT. INTEL. AGENCY, THE IC OSINT STRATEGY 2024–2026 1 (2023)

3. *See The Promise of Open-Source Intelligence*, ECONOMIST (Aug. 7, 2021), https://www.economist.com/leaders/2021/08/07/the-promise-of-open-source-intelligence [https://perma.cc/2ZZN-QRBD] (archived Sept. 14, 2024).

4. *See* Christopher Beam, *Soon, Satellites Will Be Able to Watch You Everywhere All the Time*, MIT TECH. REV. (June 26, 2019), https://www.technologyreview.com/2019/06/26/102931/satellites-threaten-privacy/ [https://perma.cc/583L-C4SB] (archived Sept. 14, 2024).

images (less than $200)[5] makes snooping more convenient.[6] Satellite imagery is one of the unique types of OSINT that can reach inaccessible areas on a consistent basis.[7] For instance, based on Australia's Defense Geospatial Intelligence (GEOINT) 2030 Strategy, the Geospatial-Intelligence Organization is authorized to collect and process a range of information, including "[i]magery and other geospatial products that are not intelligence." [8] Obviously, users should have expertise in imagery analysis to explain the consistency and confluence of the images with other OSIF, but this does not prevent inherent challenges embedded in OSIF, particularly satellite imagery.

The 1980s were considered a turning point in the commercialization of satellite imagery. In 1984, the United States Congress passed the Land Remote-Sensing Commercialization Act in which remote-sensing space systems could be operated by the private sector.[9] Under the discussion on commercial satellite imagery, in 1984, the CIA raised its concern about the involvement of the private sector in land remote-sensing satellite systems due to "the small size of the market, the public good aspects of remote sensing, and use of the data to further foreign policy objectives."[10] However, the market just needed a few years to host privately owned companies that sold high-resolution images to the US government.[11] In 1992, Congress passed the Land Remote Sensing Policy Act. Based on Section 2 of the act, "[d]evelopment of the remote sensing market and the provision of commercial value-added services based on remote sensing data should remain exclusively the function of the private sector."[12]

Now, humans live in the post-era of the limited market. In 2022, approximately "40 percent of remote sensing satellites operated in

---

5. Patrick Behrer, *Expanding the Usability of Remote Sensing Data in Development*, WORLD BANK BLOGS (Feb. 27, 2023), https://blogs.worldbank.org/en/impactevaluations/expanding-usability-remote-sensing-data-development [https://perma.cc/8LD7-RHRJ] (archived Sept. 14, 2024).

6. William J. Broad, *Private Ventures Hope for Profits on Spy Satellites*, N.Y. TIMES (Feb. 10, 1997), https://www.nytimes.com/1997/02/10/us/private-ventures-hope-for-profits-on-spy-satellites.html [https://perma.cc/MU84-535X] (archived Sept. 26, 2024).

7. *See* FRANK PABIAN, JOINT RSCH. CTR,, COMMERCIAL SATELLITE IMAGERY AS AN EVOLVING OPEN-SOURCE VERIFICATION TECHNOLOGY: EMERGING TRENDS AND THEIR IMPACT FOR NUCLEAR NONPROLIFERATION ANALYSIS 5 (2015).

8. *Geospatial Intelligence Services*, AUSTL. GOV'T DEFENCE (Jan. 3, 2024), https://www.defence.gov.au/defence-activities/products-services/geospatial-intelligence-services [https://perma.cc/2HAF-AJYK] (archived Sept. 26, 2024).

9. Land Remote-Sensing Commercialization Act, 15 U.S.C. § 401(a)(1) (1984).

10. OFF. OF TECH. ASSESSMENT, OTA-TM-ISC-20, REMOTE SENSING AND THE PRIVATE SECTOR: ISSUES FOR DISCUSSION iii (1984).

11. *See* Todd Harrison & Matthew Strohmeyer, *Commercial Space Remote Sensing and Its Role in National Security*, CTR. FOR STRATEGIC & INT'L STUD., 1 (Feb. 2022).

12. Land Remote Sensing Policy Act, 51 U.S.C. §5601(2)(15) (1992).

orbit [were] privately owned."[13] Based on the World Economic Forum's foresight, between 2023 and 2030, the Earth observation (EO) industry will contribute US$3.8 trillion to potential global gross domestic product.[14] Remote-sensing EO accounts for captured images in the visible spectrum; measurement of the geometry of natural and human-made objects; identification of the chemicals in land, water, and atmosphere, classification of land coverage and use; and assessment of atmospheric conditions.[15] Consistent with these promising achievements, Section 3(1) of the 2020 National Space Policy echoed that the United States should "facilitate the creation of new global and domestic markets for United States space goods and services, and strengthen and preserve the position of the United States as the global partner of choice for international space commerce."[16] Similarly, in 2021, the European Union passed Regulation 2021/696, highlighting that

> [F]or the Union to remain a leading international player with extensive freedom of action in the space domain, it is crucial that it encourages scientific and technical progress and supports the competitiveness and innovation capacity of space sector industries within the Union, in particular small and medium-sized enterprises (SMEs), start-ups and innovative businesses.[17]

---

13. *See* Thomas D. Taverney, *The Evolution of Space-Based ISR*, AIR & SPACE FORCES MAG. (Aug. 10, 2022), https://www.airandspaceforces.com/article/the-evolution-of-space-based-isr/ [https://perma.cc/EZU7-X8BJ] (archived Sept. 16, 2024).

14. *See* WORLD ECON. F., AMPLIFYING THE GLOBAL VALUE OF EARTH OBSERVATION INSIGHT REPORT 6 (2024).

15. *See id.* at 7.

16. "The space domain is important to the function of critical infrastructure vital to the security, economy, resilience, public health, and safety of the United States." National Space Policy, 85 Fed. Reg. 81755–58 (Dec. 16, 2020).

17. Regulation (EU) 2021/696 of the European Parliament and Council of 28 April 2021 Establishing the Union Space Programme and the European Union Agency for the Space Programme Repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU, 2021 O.J. (L 170), 69.

This proliferation brings about diverse challenges, such as cyberattacks,[18] denial of services,[19] threats to critical infrastructure,[20] and possible privacy breaches.[21] While in the past individuals had to deal with a monopoly of space espionage directed by States, nowadays, one should be concerned with "commercial spy satellites."[22] There are two main issues caused by satellite imagery. First, photos of individuals can be captured and sold.[23] It might be said that the current resolution is not high enough to show every detail of one's face, nor can satellite companies surveil for twenty-four hours.[24] That is relatively true. However, the more the technology is advanced, the more such a capability is looming. For instance, in 2014, SkyBox, a start-up company, launched its project in which high definition video clips of the Earth from space were broadcasted.[25] Similarly, another company, EarthNow, works on continuous, real-time monitoring with only a one-second delay.[26] The most recent company is Albedo, which offers aerial-quality imagery from space.[27]

---

18. *See* Mark Holmes, *The Growing Risk of a Major Satellite Cyber Attack*, VIA SATELLITE, https://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/ (last visited Sept. 26, 2024) [https://perma.cc/M5J9-PMNP] (archived Sept. 16, 2024).

19. In this case, an attack targets a satellite transponder to exploit its vulnerabilities: *See* Muhammad Usman, Marwa Qaraqe, Muhammad Rizwan Asghar & Imran Shafique Ansari, *Mitigating Distributed Denial of Service Attacks in Satellite Networks*, 31 TRANSACTIONS ON EMERGING TELECOMMS. TECHS. 1, 2 (2020).

20. *See* National Space Policy, 85 Fed. Reg. 81755–56 (Dec. 16, 2020).

21. *See* Temitope Lawal, Melanie Jackson & Eugenia Georgiades, *Privacy in the Age of Remote Sensing During Natural Disasters in Australia and Indonesia,* 4 DIGIT. L.J. 15, 21 (2023) (describing how risk of privacy breaches is increased during natural disasters).

22. Broad, *supra* note 6.

23. Sydney Shufelt, *Remote-Sensing Satellites and Privacy: Why Current Regulations Will Ultimately Fail,* AM. U. BUS. L. REV. (March 2020), https://aublr.org/2020/03/remote-sensing-satellites-and-privacy-why-current-regulations-will-ultimately-fail/ [https://perma.cc/D4PC-LASP] (archived Sept. 17, 2024).

24. *See* Beam, *supra* note 4.

25. Caleb Henry, *Skybox Imaging Releases First HD High Resolution*, SATELLITE TODAY (Dec. 27, 2013), https://www.satellitetoday.com/technology/2013/12/27/skybox-imaging-releases-first-hd-high-resolution-images-from-skysat-1/ [https://perma.cc/EZ8W-ZS2C] (archived Nov. 17, 2024). Skybox Imaging, known as Terra Bella, founded in 2009 and acquired by Google in 2014. Jeff Foust, *Planet to Acquire Terra Bella from Google*, SPACENEWS (Feb. 3, 2017) https://spacenews.com/planet-to-acquire-terra-bella-from-google/ [https://perma.cc/9SCB-Y5KT] (archived Nov. 17, 2024). In 2017, it was announced that Skybox was taken over by Planet Labs. *Google Sells Satellite Imaging Business Terra Bella to Planet Labs*, REUTERS (Feb. 3, 2017) https://www.reuters.com/article/technology/google-sells-satellite-imaging-business-terra-bella-to-planet-labs-idUSKBN15J037/ [https://perma.cc/W6Q4-SHj8] (archived Nov. 17, 2024).

26. *See* Beam, *supra* note 4.

27. *See generally Albedo*, ALBEDO SPACE CORP. (2024), https://albedo.com/ (last visited 2024) [https://perma.cc/73CE-N39P] (archived Sept. 17, 2024).

Second, satellite imagery can provide useful data on a person's everyday life. In other words, people can conduct surveillance on others from their homes.[28] Additionally, satellite imagery can have access to areas that other surveillance instruments, such as facial recognition or drones, cannot easily cover. [29] For example, the use of drones might end up trespassing on one's private property, while satellites remain in space without any concrete information about the drones' operations and capabilities. [30] Thus, it is easier to collect a targeted person's private information, which in turn opens a door toward privacy breaches. A possible solution is tightening licensing regulations to ban the sale of images on grounds of national security or public interest. However, this option, dubbed shutter control, may only be viable if the number of satellite operators is limited.[31] Currently more than one thousand EO satellites are orbiting that can gather data or capture images.[32]

This Article studies threats to privacy arising from satellite imagery. Part I elaborates on the concept of open-source investigations and the role of satellite imagery in diversifying such investigations by providing high-resolution images. It is contended that this capability can pose privacy breaches rooted in the accessibility of images. Part II addresses Australia's, the European Union's, and the United States' legal system to determine whether an effective mechanism is available to decrease the clash of privacy with OSINT. In this sense, this Article recognizes that privacy laws can substantially limit hazards associated with the deployment of satellite imagery. However, these countries diverge from a united response to privacy breaches. The discussion continues by unfolding the extent to which individual privacy is protected in the existing legal systems. When exploring privacy issues, examples may include conducting illegal surveillance and the commercialization of information gathered by satellites. [33] As such,

---

28. Natasha Bajema, *Commercial Satellites Are National Security's Next Frontier*, IEEE SPECTRUM (June 8, 2022), https://spectrum.ieee.org/commercial-satellite-imagery-national-security162 [https://perma.cc/MN9C-S9P3] (archived Sept. 17, 2024).

29. *See* William J. Broad, *When Eyes in the Sky Start Looking Right at You*, N.Y. TIMES (Feb. 20, 2024), https://www.nytimes.com/2024/02/20/science/satellites-albedo-privacy.html [https://perma.cc/4TRS-43YY] (archived Sept. 26, 2024).

30. *See id.*

31. *See* JAMES A. VEDDA, UPDATING NATIONAL POLICY ON COMMERCIAL REMOTE SENSING 1,8 (2017).

32. Nibedita Mohanta, *How Many Satellites Are Orbiting Around Earth in 2022?*, GEOSPATIAL WORLD (Apr. 20, 2023), https://www.geospatialworld.net/prime/business-and-industry-trends/how-many-satellites-orbiting-earth/ [https://perma.cc/68RB-8SD5] (archived Sept. 18, 2024).

33. *See* Cade Metz, *'Businesses Will Not Be Able to Hide': Spy Satellites May Give Edge From Above*, N.Y. TIMES (Jan. 24, 2019),

these examples provide a basis for an examination of jurisdictional data and privacy regulations to understand how such misuse is combatted by regulations in the privacy sphere.

II. SATELLITE IMAGERY AS OSIF

Although an open-source investigation is not a new phenomenon, technological innovations in the digital era, as well as the space industry, diversify its methods. Commercial satellite imagery is one of the new sources that can contribute to various investigations.[34] Nevertheless, it seems that there is a rising concern about the prevalence of high-resolution imaging and its adverse impacts on individual privacy.

A. *The Role of Satellite Imagery in OSINT and Investigations*

OSINT relies on various categories such as traditional media, the internet, publications, geolocation data, IP addresses, and commercial satellite imagery to gather information associated with national security from unclassified data.[35] Such information can be freely or commercially available.[36] Hence, OSIF represents data that is publicly available or can be acquired through the legitimate market.[37] There are three approaches to satellite imagery. In the first approach, the government is the dominant power that can invest and operate satellites.[38] The second approach gives birth to multiple private companies that can launch and administer satellite imagery as well as

---

https://www.nytimes.com/2019/01/24/technology/satellites-artificial-intelligence.html [https://perma.cc/282J-9FL2] (archived Sept. 26, 2024).

34. *See* U.N. OFF. OF THE HIGH COMM'R & UNIV. OF CAL. BERKELEY, BERKELEY PROTOCOL ON DIGITAL OPEN SOURCE INVESTIGATIONS 3 (2022) https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf (last visited Nov. 17, 2024) [https://perma.cc/JH69-9BWC] (archived Nov. 17, 2024).

35. *See* ETHICAL FRAMEWORKS IN OPEN-SOURCE INTELLIGENCE, PUBLIC-PRIVATE ANALYTIC EXCH. PROGRAM 1,7 (2022).

36. *See* BEN SCOTT, AUSTL. NAT'L UNIV. NAT'L SEC. COLL., ADAPTING AUSTRALIAN INTELLIGENCE TO THE INFORMATION AGE 1, 21 (2023) https://nsc.anu.edu.au/sites/default/files/2024-05/Ben%20Scott_AUSINT_WEB_NSC.pdf (last visited Nov. 17, 2024) [https://perma.cc/K5UK-CFxT] (archived Nov. 17, 2024).

37. *See* Heather J. Williams & Ilana Blum, DEFINING SECOND GENERATION OPEN SOURCE INTELLIGENCE (OSINT) FOR THE DEFENSE ENTERPRISE, 1, 10 (2018) ("From the perspective of the public sector, federal and/or state law governs…private sector entities experience less restrictive statutes…".) https://www.rand.org/pubs/research_reports/RR1964.html (last visited Nov. 17, 2024) [https;//perma.cc/RRM2-ZTD3] (archived Nov. 17, 2024).

38. *See, e.g.,* Cortney Weinbaum, Steven Berner & Bruce McClintock, *SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain* 1, 2 (2017) https://www.rand.org/pubs/perspectives/PE273.html (last visited Nov. 17, 2024) [https://perma.cc/NX92-2PQA] (archived Nov. 17, 2024).

sell images to potential buyers, including the government, in a legitimate market.[39] The third approach is associated with the democratization of satellite imagery in the sense that anybody can purchase images, or they are freely accessible.[40] Additionally, a competitive market exists in which innovations are promoted.[41]

Although the first approach is largely abandoned and governments tend to benefit from the second approach, the first approach still exists in some countries like North Korea.[42] In the late 1950s, the United States launched the CORONA program[43] to put a large camera into orbit. This program was run by a joint CIA-Air Force coalition without the involvement of the private sector.[44] Iran also used to exclusively consume public funds to advance satellite imaging.[45] However, in recent years, the government encouraged the private sector to invest in the design, launch, and operation of satellites.

---

39. *See id.*

40. *See id.*

41. *See* Brian Babin, *U.S. Satellite Rules Are out of Focus. It's Time for New Vision,* SPACENEWS (Apr. 27, 2017), https://spacenews.com/u-s-satellite-rules-are-out-of-focus-its-time-for-new-vision/ (arguing for US reform regarding commercial remote sensing because customers now have a world of options for such commercialization) [https://perma.cc/84JU-HPPY] (archived Sept. 18, 2024).

42. *See* CLAYTON SWOPE, KARI A. BINGEN, MAKENA YOUNG, MADELEINE CHANG, STEPHANIE SONGER & JEREMY TAMMELLEO, CLAYTON SWOPE, KARI A. BINGEN, MAKENA YOUNG, MADELEINE CHANG, STEPHANIE SONGER & JEREMY TAMMELLEO, CTR. FOR STRATEGIC & INT'L STUD., SPACE THREAT ASSESSMENT 2024 27 (2024) https://www.csis.org/analysis/space-threat-assessment-2024 (last visited Nov. 17, 2024) [https://perma.cc/HD6E-8EJX] (archived Nov. 17, 2024).

43. After multiple failures and malfunctions, eventually in August 1960, the first successful captures happened, when a canister of film dropped back through the atmosphere and was fully recovered. Corona program was one of the earliest spy satellite programs in the world. It played a pivotal role in acquiring valuable Cold War intelligence. Its mission came to an end in 1972. *See Corona Reconnaissance Satellite*, DEF. ADVANCED RSCH. PROJECTS AGENCY, https://www.darpa.mil/about-us/timeline/corona-reconnaissance-satellite (last visited Sept. 26, 2024) [https://perma.cc/RZH9-UFXR] (archived Sept. 18, 2024). In 1995, the former President of the United States Bill Clinton ordered to declassify more than 800,000 photographs collected under CORONA program. *See CORONA Photography*, HARV. UNIV., https://scholar.harvard.edu/jasonur/pages/corona-photography-1 (last visited Sept. 26, 2024) [https://perma.cc/3LPP-QQTV] (archived Sept. 18, 2024).

44. *See CORONA: America's First Imaging Satellite Program*, CENT. INTEL. AGENCY, https://www.cia.gov/legacy/museum/exhibit/corona-americas-first-imaging-satellite-program/ (last visited Sept. 26, 2024) [https://perma.cc/XFS3-9GHK] (archived Sept. 19, 2024).

45. *See* Iran Boosts Space Program Budget As Nuke Talks Go On, IRAN INTERNATIONAL, (Dec. 15, 2021) https://iranintl.com/en/20211215974897 [https://perma.cc/XV9A-XKWV] (archived Dec. 29, 2024).

Consequently, the Kowsar satellite is reportedly designed to capture high-resolution images and set to be operational by 2025.[46]

Based on the second approach, a contractual structure might be considered in which the government remains the exclusive buyer.[47] As an illustration, in 2022, after the launch of a home-grown satellite, Khayyam, the Iranian Space Agency underscored that high-resolution images might be purchased by private firms subject to request and Agency approval. [48] In another vein, following the invasion of Afghanistan in 2001, the United States put into play a contractual arrangement that allowed the government to purchase exclusively all high-resolution images related to Afghanistan from commercial operators of satellites. [49] This shutter control was substantially successful because IKONOS, launched by MAXAR Technologies Inc.,[50] was the only satellite with this capability.[51] Further, the government might reserve its right to halt imaging or restrict some critical regions.[52]

The other example is Section 1064(a) of the 1997 Defense Authorization Act. [53] This section stipulated that the Commercial Remote Sensing Regulatory Affairs can issue a license to allow commercial entities of satellite imagery to collect and distribute images related to Israel, provided that these images are "no more detailed or precise than satellite imagery of Israel that is available from commercial sources." [54] For a long time, the US Department of Commerce kept the image resolution to a 2.0 meters Ground Sample Distance (GSD) restriction.[55] However, due to the availability of better resolution through non-US commercial sources, the department was

---

46. *See* Orkhan Jalilov, *Iran Unveils Its First Satellite Designed by Private Sector*, CASPIAN NEWS (Feb. 4, 2022), https://caspiannews.com/news-detail/iran-unveils-its-first-satellite-designed-by-private-sector-2022-2-4-46/ [https://perma.cc/Q7LT-FRVY] (archived Sept. 26, 2024).

47. *See* Harrison & Strohmeyer, *supra* note 11.

48. *See Iran Benefiting from Khayyam Satellite Services*, TASNIM NEWS AGENCY, www.tasnimnews.com/en/news/2023/08/16/2940718/iran-benefiting-from-khayyam-satellite-services (last visited Sept. 26, 2024) [https://perma.cc/F3FK-4PW3] (archived Sept. 19, 2024).

49. *See, e.g.,* Duncan Campbell, *US Buys up All Satellite War Images*, GUARDIAN (Oct. 17, 2001) https://www.theguardian.com/world/2001/oct/17/physicalsciences.afghanistan [https://perma.cc/9C4F-CUCC] (archived Nov. 17, 2024).

50. *See IKONOS Satellite Imagery, Satellite Specifications* SATELLITE IMAGING CORP., https://www.satimagingcorp.com/satellite-sensors/ikonos (last visited Sept. 26, 2024) [https://perma.cc/3JAS-QJMW] (archived Sept. 19, 2024).

51. *See* VEDDA, *supra* note 31, at 8.

52. *Id.*

53. *See* National Defense Authorization Act for Fiscal Year 1997, Pub. L. No. 104–201, 110 Stat. 2653.

54. *Id.*

55. *Id.*

compelled to reduce the resolution to 0.4 meters GSD.[56] The Copernicus Programme counts as an illustration of the third approach. The project is backed by the EU and brings free access to satellite imagery.[57] While in the second approach, those who can afford images are the customers of satellite imagery,[58] in the third approach, everybody can take advantage of this source.[59] These two approaches advance non-state OSINT.[60]

Obviously, technological advancement in the space industry augments the size of the market, prompts many countries to reduce barriers to entry, and embraces more inclusive approaches.[61] This

---

56. *See* Notice of Findings Regarding Commercial Availability of Non-U.S. Satellite Imagery with Respect to Israel, 85 Fed. Reg. 44059 (July 21, 2020). Indeed, as National Defense Authorization Act for Fiscal Year 1997 does not determine any resolution threshold, the Commerce has latitude to assess available resolution regularly: License of Private Remote Sensing Space Systems, 85 Fed. Reg. 30790, at 30799 (May 20, 2020) (to be codified at 15 C.F.R. pt. 960).

57. "The vast majority of data/information delivered by Copernicus is made available and accessible to any citizen, and any organisation around the world on a free, full, and open basis." *See generally* Access to Data, COPERNICUS (last visited Dec. 29, 2024) https://www.copernicus.eu/en/access-data [https://perma.cc/V7RM-XP2L] (archived Nov. 17, 2024). *See also* CLÉMENCE POIRIER, MATHIEU BATAILLE & LARS PETZOLD, EU SPACE POLICY AND THE INVOLVEMENT OF CIVIL SOCIETY 48 (2023) https://www.eesc.europa.eu/sites/default/files/files/qe-04-23-899-en-n.pdf (last visited Dec. 29, 2024) [https://perma.cc/4KNL-82X2] (archived Nov. 17, 2024).

58. *See* Rachel McAmis, Mia Bennett, Mattea Sim & Tadayoshi Kohno*Over Fences and Into Yards: Privacy Threats and Concerns of Commercial Satellites'* 2024 PROC. PRIV. ENHANCING TECH. SYMP. 379, 390 (2024) (contending that the cost of obtaining satellite images can hinder some criminal conduct like burglaries).

59. Despite this, having limited access to up-to-date high resolution satellite images is another downside that hinders non-state OSIN investigations. *See* Eman El-Sherbiny, *Symposium on Fairness, Equality, and Diversity in Open Source Investigations: Why Tapping Into Open Source Intelligence Still Comes at a Cost for Researchers in the Global South*, OPINIO JURIS (Feb. 6, 2023) https://opiniojuris.org/2023/02/06/symposium-on-fairness-equality-and-diversity-in-open-source-investigations-why-tapping-into-open-source-intelligence-still-comes-at-a-cost-for-researchers-in-the-global-south/ [https://perma.cc/RS9Z-2GUM] (archived Nov. 17, 2024).

60. *See* CLÉMENCE POIRIER, MATHIEU BATAILLE & LARS PETZOLD, EU SPACE POLICY AND THE INVOLVEMENT OF CIVIL SOCIETY 48 (2023); *see also The Promise of Open-Source Intelligence*, ECONOMIST (Aug. 7, 2021), https://www.economist.com/leaders/2021/08/07/the-promise-of-open-source-intelligence [https://perma.cc/2ZZN-QRBD] (archived Sept. 14, 2024); *see also Resources for Finding and Using Satellite Images*, GLOB. INVESTIGATIVE JOURNALISM NETWORK (Sept. 16, 2023) https://gijn.org/resource/resources-for-finding-and-using-satellite-images/ [https://perma.cc/HB2B-D2E7] (archived Nov. 17, 2024).

61. KARI A BINGEN, DAVID GAUTHIER & MADELEINE CHANG, GOLD RUSH: THE 2024 COMMERCIAL REMOTE SENSING GLOBAL RANKINGS 1 (October 2024), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-09/241001_Bingen_Gold_Rush.pdf?VersionId=FtAy0I3xBa6EHM.DQJFHxJtZo3W0U1IE [https://perma.cc/622T-2WBC] (archived Nov. 17, 2024). "[A]ctive government support

movement substantially aligns with the Outer Space Treaty. The treaty points out that "the exploration and use of outer space shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind."[62] When this rule was adopted, a vast majority of people could not have access to space, unlike the convenience of public streets in residential areas.[63] Despite this, it should be noted that commercial satellite imaging is a game changer and becomes one of the instances of "the province of all mankind" because it provides individuals with access to images from space as well as the private sector's investments in the space industry.[64]

Outstanding progress in launching reusable rockets, crafting smaller satellites, and exploiting low-earth orbit [65] dramatically reduces the cost of satellite imagery for certain nations and increases the use of such techniques in both OSINT and non-state investigations.[66] These capabilities enable analysts to find out new military movements in a hostile country. [67] Additionally, remote sensing data provides better insights into natural disasters or market conditions. For instance, changes in maritime or truck transportation might indicate that the market is rising or declining in a given region.[68] Satellite imagery can also be valuable evidence in cases of dispute between two neighboring countries. As an illustration, Afghanistan and Iran have been dealing with a conflict over Iran's share of the Hirmand River. [69] Afghanistan claimed that, due to drought and

---

has tremendously encouraged the growth of commercial sales of imagery in a number of countries.".; Yahya A Dehghanzada & Ann M Florini, SECRETS FOR SALE: HOW COMMERCIAL SATELLITE IMAGERY WILL CHANGE THE WORLD, 17 (2000) https://carnegieendowment.org/research/2000/03/secrets-for-sale-how-commercial-satellite-imagery-will-change-the-world?lang=en> [https://perma.cc/B9TV-7D2M] (archived Nov. 17, 2024); *see also* Victoria Samson, *The Complicating Role of the Private Sector in Space*, 78 BULL. ATOMIC SCIENTISTS 6, 7 (2022).

62. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 205 (adopted October 10, 1967) [hereinafter Principles Governing the Activities].

63. *See* Lisa J. Steele, *The View from on High: Satellite Remote Sensing Technology and the Fourth Amendment*, 6 BERKELEY HIGH TECH. L.J., 317, 327 (1991).

64. *See* Principles Governing the Activities, *supra* note 62.

65. This article does not aim to unfold the specifications of low-earth orbit and current projects on the advancement of reusable rockets. *See* Matin Pedram & Eugenia Georgiades, *The Role of Regulatory Frameworks in Balancing Between National Security and Competition in LEO Satellite Market*, 14 J. NAT'L SEC. L. & POL'Y. 179, 185–90 (2024).

66. *See* Harrison & Strohmeyer, *supra* note 11.

67. *See id.*

68. *See id.*

69. Holly Dagres, *Iran and Afghanistan Are Feuding over the Helmand River. The Water Wars Have No End in Sight*, ATL. COUNCIL (July 7, 2023), https://www.atlanticcouncil.org/blogs/iransource/iran-afghanistan-taliban-water-helmand/ [https://perma.cc/Z9U7-XM3A] (archived Nov. 17, 2024).

weather events, there is not enough water in the dams.[70] Despite this, in 2023, Iran released satellite images to negate the claims that the dams in Afghanistan do not hold sufficient water to be allocated to Iran based on the 1973 Helmand River Treaty.[71] The International Criminal Court (ICC) prosecution used satellite images as evidence of war crimes, namely the destruction of heritage sites in Mali.[72] In another vein, many journalists are utilizing images from commercial satellite operators in their reporting on the war in Ukraine,[73] and as the ICC investigates possible crimes committed by Russia, there is much discussion on the use of satellite images as investigative tools.[74]

Further, this abundant accessibility makes it possible for independent institutions and individuals to undercut the monopoly of government agencies in bringing forward their own interpretations.[75] In particular, commercial satellite imagery is a component of OSIF

---

70. *See* Afghan Witness, *The Water Rights Dispute behind Rising Afghan-Iran Tensions*, CTR. FOR INFO. RESILIENCE (June 2, 2023), https://www.info-res.org/post/the-water-rights-dispute-behind-rising-afghan-iran-tensions [https://perma.cc/3E7Z-SV9E] (archived Sept. 19, 2024).

71. The Afghan-Iranian Helmand-River Water Treaty art. V.,13 March 1973; *see also* Farnaz Shirani Bidabadi & Ladan Afshari, *Human Right to Water in the Helmand Basin: Setting a Path for the Conflict Settlement between Afghanistan and Iran* 16(2) UTRECHT L. REV.150, 156 (2020).

72. "The Prosecution will use satellite images, photographs, videos and other material gleaned from the Internet which are included on the list of our evidence material to show the situation of the mausoleums before, during and after the destruction, including the participation of the accused." The Prosecutor v. Ahmad Al Faqi Al Mahdi (Transcript), ICC-01/12-01/15 at ¶ 41. (Sept. 27, 2016). The most recent case where satellite images were widely used to identify the scale of demolishment of residential areas is Ukraine. The Independent International Commission of Inquiry on Ukraine relied on satellite images to demonstrate the magnitude of destruction in Mariupol. *See* Jonathan W. Hak & Sabrina K. Rewald, *The Satellite Era: How Earth Observation Data Is Being Mobilized as Potential Digital Evidence*, EJIL: TALK! (July 1, 2024) https://www.ejiltalk.org/the-satellite-era-how-earth-observation-data-is-being-mobilized-as-potential-digital-evidence/ [https://perma.cc/XNS7-KQTH] (archived Dec. 29, 2024).

73. *See* Bryan Bender, *Satellite Companies Join the Hunt for Russian War Crimes*, POLITICO (Apr. 6, 2022), https://www.politico.com/news/2022/04/06/satellite-russian-war-crimes-00023386 [https://perma.cc/6HU4-CPMV] (archived Sept. 27, 2024).

74. *See* Denise Chow & Yulia Talmazan, *Watching from Space, Satellites Collect Evidence of War Crimes*, NBC NEWS (May 3, 2022), https://www.nbcnews.com/science/science-news/ukraine-satellites-war-crimes-rcna26291 [https://perma.cc/8YGX-3F3T] (archived Sept 19, 2024); *see also* Mariel Borowitz, *War in Ukraine Highlights the Growing Strategic Importance of Private Satellite Companies – Especially in Times of Conflict*, CONVERSATION (Aug. 15, 2022), http://theconversation.com/war-in-ukraine-highlights-the-growing-strategic-importance-of-private-satellite-companies-especially-in-times-of-conflict-188425 [https://perma.cc/UT8Y-BEMN] (archived Sept. 19, 2024).

75. *See* Sam Roggeveen, *Open Sources and the Future of Spying*, LOWY INST. (Mar. 20, 2024), https://www.lowyinstitute.org/the-interpreter/open-sources-future-spying [https://perma.cc/B9C9-LA27] (archived Sep. 19, 2024).

that rivals a State's narrative and decentralizes the concept of OSINT. The notorious illustration is the PS752 flight shot down by the Islamic Republic Guard Corps on January 8, 2020, outside Tehran.[76] At first, the Iranian government explained that it was a crash without the involvement of a missile attack.[77] However, analysts brought OSIF, such as a video related to the crash, alongside satellite images of the location, demonstrating that the aircraft was targeted by a rocket.[78] Ultimately, the former president of the Islamic Republic of Iran, Hassan Rouhani, admitted to the crash, marking it as "a disastrous mistake."[79] It seems that satellite imagery is turning into a pivotal component in addressing national security challenges, gathering information, and enhancing independent investigations.[80]

B. *The Clash of Privacy Concerns with Satellite Imagery*

Despite this multiplicity, satellite imagery can simplify the identification of people, which raises questions about privacy protections and applicable regulations. [81] In 2013, the United Nations General Assembly acknowledged that

> [T]he rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection, which may violate or abuse human rights, in particular the

---

76. *See Open-Source Intelligence Challenges State Monopolies on Information*, ECONOMIST (Aug. 7, 2021), https://www.economist.com/briefing/2021/08/07/open-source-intelligence-challenges-state-monopolies-on-information [https://perma.cc/ZM2D-WLGH] (archived Sept. 19, 2024).

77. *See* Phil Helsel & Ali Arouzi, *Iran Admits to Unintentionally Shooting down Ukrainian Plane*, NAT'L BROAD. CO. NEWS (Jan. 10, 2020), https://www.nbcnews.com/news/world/iranian-military-says-it-unintentionally-shot-down-ukrainian-plane-n1113996 [https://perma.cc/43Y8-E2RU] (archived Sept. 19, 2024).

78. *See Open-Source Intelligence Challenges State Monopolies on Information, supra* note 76.

79. *See "Disastrous Mistake": Iran Admits It Shot Down Ukrainian Plane*, AL JAZEERA (Jan. 11, 2020), https://www.aljazeera.com/news/2020/1/11/disastrous-mistake-iran-admits-it-shot-down-ukrainian-plan [https://perma.cc/8AUR-TWVN] (archived Sept. 19, 2024).

80. *See* Cristiana Santos & Lucien Rapp, *Satellite Imagery, Very High-Resolution and Processing-Intensive Image Analysis: Potential Risks Under the GDPR*, 44 AIR & SPACE L. 275, 275–76 (2019).

81. Megan M. Coffer, *Balancing Privacy Rights and the Production of High-Quality Satellite Imagery*, 54 ENV'T SCI. & TECH. 6453, 6453 (2020).

> right to privacy, as set out in article 12 of the Universal Declaration of Human Rights.[82]

The resolution unveiled two concerns related to technological advancements: government omnipotence and individuals' enhanced options to spy on others. Article 12 of the Universal Declaration of Human Rights of 1948 underscores that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence . . . [e]veryone has the right to the protection of the law against such interference or attacks." [83] It seems that individual privacy is of the utmost importance in human rights, and countries are committed to employing protective and preventive measures to shield it from violations.

Nonetheless, there may be many circumstances in which individuals' OSIF, including images from their properties or themselves, are misused, but this cannot be a cornerstone to enlarge the concept of privacy to protect any type of OSIF. [84] Thus, it is necessary to strike a balance between privacy concerns and the use of OSIF in OSINT or non-state investigations. For this, privacy should be identified as "that aspect of social order by which persons control access to information about themselves."[85] In this sense, one can legitimately expect that privacy laws should protect personal images on the grounds of dignity and autonomy.[86] It can be suggested that the protection of personal images amounts to the protection of private life.[87] It should be taken into account that "[e]ven though information may be publicly available, it does not mean that there are no privacy implications in its collection and use."[88] As the Supreme Court of California in *Shulman v. Grp. W Prod. Inc.* maintained,

> Our secrets, great or small, can now without our knowledge hurtle around the globe at the speed of light, preserved indefinitely for future recall in the electronic limbo of computer memories. These technological and economic

---

82. G.A. Res. 68/167, at 1 (Dec. 18, 2013).

83. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at art. 12 (Dec. 10, 1948).

84. *See* Eugenia Georgiades, *A Right That Should've Been: Protection of Personal Images on the Internet*, 61 L. REV. FRANKLIN PIERCE CTR. FOR INTELL. PROP. 275, 300 (2020).

85. Charles Fried, *Privacy*, 77 YALE L.J. 475, 493 (1968).

86. *See* Georgiades, *A Right That Should've Been: Protection of Personal Images on the Internet*, *supra* note 84, at 305.

87. *See id.* at 309.

88. U.N. OFF. OF THE HIGH COMM'R & UNIV. OF CAL. BERKELEY, *supra* note 34, at 12.

> changes, in turn, have made legal barriers more essential to the preservation of our privacy.[89]

Accordingly, aerial surveillance conducted by state agencies, like the police, can be deemed plausible, while persistent surveillance through satellites may count as GPS monitoring and breach of privacy expectations.[90] In the case of non-state, open-source investigations, investigators and satellite operators should consider one's legitimate expectations of privacy on various occasions. The question is whether a person's legitimate expectations can be applied to satellite imagery, where such images lack people's facial details. For instance, the images can contain information about one's backyard or the shape of the house. Generally, given the fact that satellite imaging does not aggress against people's possession and enjoyment of their properties, the conventional arguments grounded on trespassing or private nuisance cannot curb satellite imagery hazards.[91] Moreover, when satellites are launched, they stay in orbit without bringing about any noise, pollution, or harm. Thus, trespass and nuisance cannot constitute a solid ground for privacy protection.[92]

Nevertheless, an image belonging to one's property can be blended with supplementary information, resulting in the identification of that person or a group of people.[93] Analogously, taking photos of people in their cars or homes without their consent might infringe upon privacy, while capturing their mere presence in public does not count as a privacy breach.[94] This issue can be exacerbated if the proliferation of the satellite imagery and a vast investment in this segment are taken into account. In this sense, due to the lack of cooperation among multiple players, satellite operators, hostile countries, and non-state investigators, the environment tends to be more noncooperative,[95] meaning that players are not inclined to reach a collaborative scheme.[96] Thus, each player pursues its interests and preferences,

---

89. Shulman v. Group W. Productions, Inc. 18 Cal. 4th 200, 243–44 (1998) (Kennard J., concurring).

90. *See* John Pavletic, *The Fourth Amendment in the Age of Persistent Aerial Surveillance*, 108 J. CRIM. L. & CRIMINOLOGY 171, 195–96 (2018).

91. *See* Brian Craig, *Online Satellite and Aerial Images: Issues and Analysis*, 83 N.D. L. REV. 547, 559 (2007).

92. *See id.* at 560.

93. *See* U.N. OFF. OF THE HIGH COMM'R & UNIV. OF CAL. BERKELEY, *supra* note 34, at 12.

94. *See* Craig, *supra* note 91, at 562.

95. While extraterritorial impacts of satellite imagery breed significant concerns predominantly due to diverging viewpoints and conflicting interests of countries, it requires a distinct paper to elaborate on the concerns and consider both cooperative and noncooperative games on the international level.

96. *See* John Nash, *Non-Cooperative Games*, 54 ANNALS MATHEMATICS 286, 295 (1951).

while its decisions on the capture, use, and dissemination of high-resolution images can influence other players across the world.[97] In the absence of cooperation, any government that takes the initiative to tighten the regulation on satellite imagery or ban satellite commercialization hampers innovation without any positive legal results.[98] Hence, it seems that the legal solution should align with the competitive market, monitoring the use of OSIF and cracking down on unnecessary disclosure of one's life.

In the next Part, privacy laws of three distinct jurisdictions, Australia, the European Union, and the United States, are examined to determine whether adequate safeguards are in place and to what extent these legal systems can pass the abovementioned test.

III. PRIVACY LAWS AND SATELLITE IMAGERY

In 2017, a fitness tracking company, Strava, released its visualization map, which was built based on users' tracked activities.[99] This information ended up revealing the locations of military bases and spy outposts worldwide.[100] Such a capability has prompted governments to tighten regulations on the use of images on the grounds of national security or public interest.[101] Restrictive measures like shutter control might effectively preserve national security interests, but due to an unlimited number of individuals, multiple movements across the world, and varying jurisdictions, the protection of privacy is more sophisticated and requires a progressive approach. Thus, privacy laws may provide a viable safeguard.

---

97. *See* ERIC VAN DAMME, CTR. FOR ECON. RSCH., NON-COOPERATIVE GAMES 2 (2000).

98. *See generally* Dustin L. Hayhurst Sr. & John M. Colombi, *Game-Theoretic System Design in the Development of Space Power*, 35 AIR & SPACE POWER J. 20, 22, 31–32 (2021) (discussing how game theory can inform governmental policy choices in the development of space technology).

99. Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret US Army Bases,* GUARDIAN (Jan. 28, 2018), https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases [https://perma.cc/8W4T-JD6T] (archived Sept. 27, 2024).

100. *Id.*

101. Hannah Kannegieter, *Privacy and Veracity Implications of the Use of Satellite Imagery from Private Companies as Evidence in Human Rights Investigations*, HARV. HUM. RTS. J. (Nov. 29, 2023), https://journals.law.harvard.edu/hrj/2023/11/privacy-and-veracity-implications-of-the-use-of-satellite-imagery-from-private-companies-as-evidence-in-human-rights-investigations/ [https://perma.cc/ZR6G-7WX7] (archived Oct. 10, 2024).

A. *Australia*

1. Privacy Laws

In Australia, the backbone of privacy protection is established by tort law and the Privacy Act 1988 (Commonwealth).[102] In the case of satellite imagery, breach of confidence seems to be the most relevant tort.[103] In *Coco v. AN Clark (Engineers) Ltd.*, it is established that information should qualify as confidential.[104] Hence, there should be circumstances associated with an obligation of confidence and an unauthorized use of this information committed by the receiving party.[105] Consequently, this tort is limited to the revelation of images showing an intimate or sexual nature; therefore, there is no room to protect individuals in public or visible areas.[106]

Breach of confidence is expanded to include a test for a reasonable expectation of privacy.[107] In *Doe v. Australian Broad. Corp.*, the Country Court of Victoria posited that "confidential or private information is information in respect of which a person has a reasonable expectation of privacy, and that confidence or privacy is breached if a person publishes the information in circumstances where they knew or ought to have known of that reasonable expectation of privacy."[108] Nonetheless, the public interest is an exception to the duty of confidence.[109] In *Doe v. Australian Broad. Corp.*, the Country Court of Victoria maintained that the publication of information is wrong when it is prohibited to be published and the shared information is unlikely to be the point of public interest.[110] In this sense, two competing interests can be identified: the public interest in disclosure and the public interest in confidentiality.[111] Subsequently, "the

---

102. It should be noted that the said Act does not hinder state legislatures to pass their own privacy laws. *See generally* Eugenia Georgiades, *Blind Hope, Magnificent Delusions: The Need for Privacy Protection for Personal Images Uploaded on Social Networks*, 43 EUR. INTELL. PROP. REV. 148, 148 (2021).

103. Des Butler, *Drones and Invasions of Privacy: An International Comparison of Legal Responses* 42 UNIV. NEW S. WALES L.J. 1039, 1046 (2019).

104. Coco v. A.N. Clark (Engineers) Ltd [1969] EWHC (Ch) 41, 47 (Eng.).

105. *Id*.

106. Georgiades, *Right That Should've Been: Protection of Personal Images on the Internet*, *supra* note 84, at 301.

107. *See* Butler, *supra* note 103, at 1047; *see generally* Eugenia Georgiades, *Ignoring the Call for Law Reform: Is It Time to Expand the Scope of Protection for Personal Images Uploaded on Social Networks?* 26 TORT L. REV. 166 (2019) (discussing the need for reformation of Australian law to better protect personal images and whether expansion of the common law is the correct way to address the issue).

108. Doe v. Australian Broadcasting Corporation [2007] VCC 281, 1, 38 (Austl.).

109. Jason Pizer, *The Public Interest Exception to the Breach of Confidence Action: Are the Lights About to Change?* 20 MONASH UNIV. L. REV. 67, 67 (1994).

110. *Doe* [2007] VCC 281 at 54.

111. Pizer, *supra* note 109, at 68.

disclosure of an iniquity"[112] such as a "crime, civil wrong, or serious misdeed of public importance" [113] cannot count as a breach of confidence.[114]

Based on the abovementioned analysis, it seems that in the case of satellite imagery, images taken out of private areas or places that lack the reasonable expectation of privacy can be shared by satellite operators, in addition to the use of non-state investigators. However, it is obvious that such images are deprived of one's consent. Still, these images can be deemed confidential because, regardless of a person's presence in public, one has no participation in taking and sharing images.[115] Hence, the Privacy Act 1988 can be incorporated into the analysis to bridge the gap between privacy concerns arising from satellite imagery and the lack of a comprehensive protection. According to Section 6 of the Privacy Act 1988, any information relating to an identified individual, or who is reasonably identifiable, is specified as personal information.[116] Personal information includes sensitive data such as religious beliefs, ethnicity, political opinions, membership in a political or trade association, and health information.[117]

Based on Section 6(C) of the Privacy Act 1988, government agencies and private organizations [118] with more than $3 million annual turnover must comply with the requirements of the Privacy Act 1988.[119] With this threshold, non-state, open-source investigators may be exempted from the requirements of the act, even though satellite operators are likely required to conform to the Privacy Act 1988. Section 5(B) of the act expands Australia's jurisdiction, introducing extraterritorial operations.[120] Accordingly, if a satellite operator has an Australian link, its activities must be consistent with the act.[121] Collecting personal information in Australia or carrying on business in Australia are among some of the instances of an Australian link.[122]

---

112. Butler, *supra* note 103, at 1047.

113. *Id.*

114. Pizer, *supra* note 109, at 70.

115. *See* Georgiades, *Right That Should've Been: Protection of Personal Images on the Internet*, *supra* note 84, at 317.

116. *See Privacy Act 1988* (Cth) s 6 (Austl.) (amended 2024).

117. *See id.* at s 6C.

118. Private organizations represent individuals, body corporates, partnerships, any other unincorporated associations, or trusts. *See id.*

119. They are dubbed APP entities. THE OFF. OF THE AUSTL. INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES 18 n.B.25 (2019).

120. *Privacy Act 1988* (Cth) s 5B(1) (Austl.). ("This Act, a registered APP code and the registered CR code extend to an act done, or practice engaged in, outside Australia and the external Territories by an organization, or small business operator, that has an Australian link").

121. *Id.*

122. *Id.* at s 5B(3).

For simplicity, it is hypothesized that a satellite operator holds, uses, discloses, and collects images of Australian individuals or anything inside the Australian territory. Hence, it must be ensured that the operation does not infringe on one's right to privacy. Consistent with the Australian Privacy Principles Guidelines 2019 (the Guidelines), an APP entity holds personal information when it has a possessive or controlling relationship with an image of a person.[123] Using personal information unveils a situation in which the entity "handles or undertakes an activity with the information, within the entity's effective control."[124] Disclosure of personal information occurs when an APP entity provides external third parties with access to information. However, in some cases, the entity might lose its effective control over the information which in turn enables external third parties to exploit it.. For instance, personal information might become available on the internet in the sense that everyone can download data.[125] In this sense, a satellite operator might publish images freely, sell them, or accidentally release images of a person captured by satellites.[126]

For free access or a noncommercial purpose, the satellite operator might go below the turnover threshold; therefore, the dissemination of images is exempted from the requirements of the Privacy Act 1988.[127] In the case of commercial satellite imagery, although satellites are allowed to take high-resolution images, the dissemination or transfer to users, like non-state investigators, must comply with privacy considerations.[128] Further, if these images are used for journalism by a media organization, such an organization is exempted from the requirements of the Privacy Act 1988.[129]

Nevertheless, for the satellite operator, the limitation persists. Thus, images of persons cannot be taken or must be masked. As an illustration, the Murray-Darling Basin Authority (MDBA) is authorized under the Water Act 2007 (Commonwealth) to collect and

---

123. *See* THE OFF. OF THE AUSTL. INFO. COMM'R, INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES, *supra* note 119, at ¶ 6.7.

124. *Id.* ¶ 6.8.

125. *Id.* ¶ 6.9 & 6.10.

126. *Id.* ¶ 6.10.

127. *See* above. *See also* Privacy Act 1988, sec 6(c).

128. Georgiades, *Blind Hope, Magnificent Delusions: The Need for Privacy Protection for Personal Images Uploaded on Social Networks*, *supra* note 102, at 150.

129. *See Privacy Act 1988* (Cth) s 7B(4) (Austl.). ("An act done, or practice engaged in, by a media organisation is exempt for the purposes of paragraph 7(1)(ee) if the act is done, or the practice is engaged in: (a) by the organization in the course of journalism; and (b) at a time when the organization is publicly committed to observe standards that: (i) deal with privacy in the context of the activities of a media organization (whether or not the standards also deal with other matters); and (ii) have been published in writing by the organization or a person or body representing a class of media organizations.").

use satellite images.[130] However, the MDBA emphasizes that the resolution of the collected images is ten meters. This means that an object which is smaller than ten meters cannot be identified. It is self-evident that individuals are recognizable in such an image.[131] In another vein, if satellite images reveal other personal information, like one's political, religious, or commercial affairs, satellite operators must employ protective measures to curb data disclosure because such information is characterized as sensitive information.[132]

2. Legal Constraints of Data Collection

Section 3.1 of the Privacy Act 1988 (Commonwealth) differentiates sensitive information from personal information, ruling that an APP entity is permitted to collect personal information when it is reasonably necessary for one or more of the entity's functions or activities.[133] According to the Guidelines, the collection of personal information arises from primary or secondary purposes.[134] The primary purpose is "the specific function or activity for which the entity collects the personal information."[135] If satellite imagery aims to capture high-resolution images, one's identity may be recognizable; therefore, the satellite operator must justify such images as "reasonably necessary."[136]

According to the Guidelines, reasonableness is an objective test, which considers an informed person's expectations toward the collection of personal information in certain circumstances.[137] It entails that there should be some facts, prompting "state of mind in a reasonable person."[138] As an illustration, Section 21 of the Law Enforcement (Powers and Responsibilities) Act 2002 (NSW) maintains that a police officer has a right to stop, search, and detain a person on reasonable grounds, such as carrying a prohibited drug or possessing

---

130. *Privacy Collection Notice for Geospatial Satellite Images*, AUSTL. GOV.: MURRY-DARLING BASIN AUTH. (June 27, 2023), https://www.mdba.gov.au/publications-and-data/maps-and-spatial-data/geospatial-data-services-request/privacy-collection [https://perma.cc/3UPJ-TCV2] (archived Sept. 29, 2024).

131. *Id.*

132. *See Privacy Act 1988* (Cth) s 6 (Austl.).

133. THE OFF. OF THE AUSTL. INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES, *supra* note 119, at ¶ 3.1.

134. THE OFF. OF THE AUSTL. INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES, *supra* note 119, at ¶ 6.12.

135. *Id.* at ¶ B.101.

136. *Id.* at ¶ B.103.

137. *Id.* at ¶ B.105.

138. George v. Rockett, [1990] HCA 26 (Austl.).

a dangerous object in a public place where a relevant offense took place or might take place.[139]

An entity's functions comprise current and future planned activities.[140] Imagery could be ascribed to a satellite operator's function if such an activity was recognized and licensed by the Australian authorised agency.[141] However, it cannot be taken for granted that the satellite operator can collect and disseminate individuals' images simply on grounds of its planned function. If satellite imaging is associated with the collection of sensitive information,[142] the satellite operator must obtain a person's consent in addition to passing the reasonableness test.[143] Despite this, getting almost every individual's consent in any given territory is impossible. Based on Section 16 (A)(1) of the Privacy Act 1988, an APP entity is allowed to collect, disclose, and use personal information once it is unreasonable or impracticable to get a person's consent.[144] Given the nature of satellite imagery, which makes consent costly, time-consuming, and inconvenient, on most occasions, it seems that satellite imaging can be operated without getting a person's consent.[145]

Section 3.5 of the Privacy Act 1988 stipulates that the collection of personal information must be done through fair and lawful means.[146] Lawfulness represents that satellite imagery must be consistent with the relevant laws and regulations.[147] For instance, high-resolution satellite images should not be associated with trespassing on a person's

---

139. *See* Law Enforcement (Powers and Responsibilities) Act 2002, c. 21 (Wales).

140. THE OFF. OF THE AUSTL. INFO. COMM'R, INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES, *supra* note 119, at 3.13.

141. Since satellites use radio spectrum to transmit data to the ground station, Australian Communication and Media Authority (ACMA) must allocate and license satellite operation: *Radiocommunications Act 1992*, sec 60. Further, if the satellite is supposed to be launched from anywhere by an Australian citizen or through the Australian territory, the launch must be approved by the Minister for Industry, Science, and Technology: *Space (Launches and Returns) Act 2018*, sec 4.

142. *See Privacy Act 1988* (Cth) s 6(1) (Austl.). ("Sensitive information means information or an opinion about an individual's:(i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates").

143. *See* THE OFF. OF THE AUSTL. INFO. COMM'R, INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES, *supra* note 119, at ¶ 3.3.

144. *Privacy Act 1988* (Cth) s 16A(1) (Austl.).

145. *See* THE OFF. OF THE AUSTL. INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES, *supra* note 119, at ¶ C.6.

146. *Id.,* at ¶ 3.5.

147. *See id.,* at ¶ 3.61.

private property[148] or breach of confidence.[149] Fairness identifies circumstances where the collection of information occurs in the absence of one's knowledge.[150]

Based on the abovementioned argument, satellites spin and capture images when few people are aware of them. Therefore, if a person's identity becomes evident or can reasonably be determined by satellite images,[151] the satellite operator must employ precautionary measures alongside data collection.[152] In this respect, the entity must put in place an up-to-date APP privacy policy explaining how the entity handles personal information.[153] Additionally, the privacy policy should reflect on the purposes for which personal information is gathered and how individuals can have access to their personal information and complain about any breaches of the privacy regulations.[154] The privacy policy should also make it clear whether personal information is disclosed to overseas recipients.[155]

It seems that the collection of personal information is unlikely to constitute the functionality of a satellite operator, but it is impractical to exclude personal information, such as a person's appearance, car, and private property, during satellite imaging. Accordingly, satellite imaging gathers some personal or sensitive information that does not necessarily align with the function of the entity. Thus, the satellite operator must destroy or anonymize captured images to increase the likelihood of complying with the Privacy Act 1988 (Cth) and the Guidelines.[156] Otherwise, the satellite operator should justify its reasonableness and necessity.[157] If a foreign business includes a satellite operator whose main business is out of Australia but the operator "acts within Australia," it is deemed to comply with the Privacy Act 1988.[158] For instance, Clearview AI, a US entity without any office in Australia, collected facial images of Australian people

---

148. *See id.*

149. *See* Georgiades, *A Right That Should've Been: Protection of Personal Images on the Internet*, *supra* note 84, at 301.

150. *See, e.g.,* THE OFF. OF THE AUSTL. INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES, *supra* note 119, at ¶¶ 3.62–.63.

151. *See* Georgiades, *Blind Hope, Magnificent Delusions: The Need for Privacy Protection for Personal Images Uploaded on Social Networks*, *supra* note 102, at 149–51.

152. *Privacy Act 1988* (Cth) s 16A (Austl.).

153. THE OFF. OF THE AUSTL. INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES, *supra* note 119, at ¶ 1.2.

154. *Id.* at ¶ 1.15.

155. *Id.*

156. *Id.* at ¶¶ 4.3, 4.14.

157. THE OFF. OF THE AUSTL. INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES, *supra* note 119, at ¶ B.115.

158. THE OFF. OF THE AUSTL. INFO. COMM'R, AUSTRALIAN PRIVACY PRINCIPLES GUIDELINES, *supra* note 119, at ¶ B.17.

from the internet. The Office of the Australian Information Commissioner accused the entity of noncompliance with the Privacy Act 1988, conducting a legal investigation.[159]

B. *The European Union*

1. Privacy Laws

Article 8 of the European Convention on Human Rights (ECHR) states that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[160] Article 8 of the ECHR is applicable to multiple situations involving satellite imagery. For instance, when a satellite operator constantly collects and processes data associated with one's identity or property, monitors one's life, or shares high-resolution images of a person, it interferes with the right to privacy embedded in Article 8 of the ECHR.[161]

Based on Article 16 of Resolution 428 passed by the Parliamentary Assembly, the right to privacy represents "the right to live one's own life with a minimum of interference."[162] Consequently, Article 8 accounts for situations like unauthorized publication of private photos, protection against misuse of private communications, and protection from disclosure of confidential information.[163] In 1998, in response to the proliferation of communication technologies, Resolution 1165 incorporated "the right to control one's own data" into the definition.[164] The right to privacy encapsulated in Article 8 obliges the State to

---

159. "Clearview AI, through its collection of facial images and biometric templates from individuals in Australia using a facial recognition technology, contravened the Privacy Act, and breached several Australian Privacy Principles (APPs) in Schedule 1 of the Act, including by collecting the sensitive information of individuals without consent in breach of APP 3.3 and failing to take reasonable steps to implement practices, procedures and systems to comply with the APPs." *Statement on Clearview AI',* OAIC (Aug. 21, 2024) https://www.oaic.gov.au/news/media-centre/statement-on-clearview-ai [https://perma.cc/V7KK-9YXS] (archived Dec. 29, 2024). OAIC dropped the case in August 2024. *See* Josh Taylor, *Privacy Regulator Drops Pursuit of Clearview AI as Greens Call for More Scrutiny on Use of Australians' Images*, GUARDIAN (Aug. 21, 2024) https://www.theguardian.com/technology/article/2024/aug/21/privacy-regulator-drops-pursuit-of-clearview-ai-over-use-of-australians-images-in-facial-recognition-tech-ntwnfb [https://perma.cc (archived Nov. 17, 2024).

160. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221 (entered into force Sept. 3, 1953) (amended Aug. 1, 2021 by Protocol No. 15).

161. *See* Santos & Rapp, s*upra* note 80, at 288.

162. Eur. Consult. Ass., *Declaration on Mass Communication Media and Human Rights,* 18th Sess., Doc. No. 428 (1970).

163. *Id.*

164. Eur. Consult. Ass., *Right to Privacy*, 24th Sess., Doc. No. 1165 (1998).

safeguard the right to privacy.[165] For instance, when a domestic law allows a degree of privacy disclosure, it should be interpreted with respect to Article 8.[166]

In *Von Hannover v. Germany*, the plaintiff, who was a member of the Prince Rainier III of Monaco family, sought to stop the publication of photos related to her private life in the press.[167] Some photos were taken during her holiday in Zurs/Arlberg and when she went shopping at the market.[168] Based on Section 23(1) of the Copyright Act, the German courts held that the plaintiff is a person of contemporary society who should tolerate the publication of photos.[169] However, The European Court of Human Rights (ECtHR) postulated that laws must be "interpreted narrowly to ensure that the State complies with its positive obligation under the Convention to protect private life and the right to control the use of one's image."[170]

Further, Resolution 1165 emphasized that freedom of expression and the right to privacy amount to fundamental rights in a democratic society.[171] However, neither of those rights is absolute.[172] In the case of open-source investigations, these two fundamental rights might intersect. Hence, there should be a balance between these competing interests. It seems that the ECtHR relies on general interest and legitimate expectations as balancing measures.[173] On some occasions, individuals can plausibly expect privacy. A debate of general interest is a force that makes the publication permissible. In *Krone Verlag GmbH & Co. KG v. Austria*, the ECtHR held that the protection of privacy must "be weighed against the interests of open discussion of political issues."[174] In this case, an Austrian newspaper published an article with a picture of a politician who allegedly received three salaries.[175] Following the politician's complaint, the Supreme Court of

---

165. "…although the essential object of Article 8 (art. 8) is to protect the individual against arbitrary interferences by the public authorities with his or her exercise of the right protected, there may in addition be positive obligations inherent in an effective 'respect' for private life." Stjerna v. Finland Eur. Ct. H.R. (1994) para 38.

166. See Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 (adopted Sept. 3, 1953) (amended Aug. 1, 2021 by Protocol No. 15). Case of Von Hannover v. Germany Eur. Ct. H.R. (2005).

167. Case of Von Hannover v. Germany Eur. Ct. H.R. ¶ 9 (2005).

168. *Id.* at ¶¶ 13, 14.

169. *Id.* at ¶ 19.

170. *Id.* at ¶ 72.

171. Eur. Consult. Ass., *Right to Privacy*, 24th Sess., Doc. No. 1165 (1998).

172. *Id.*

173. Ian Cram, *The Right to Respect for Private Life: Digital Challenges from a Comparative-Law Perspective* (European Parliamentary Research Service, October 2018) 18. *See also* Case of Oberschlick v. Austria, Eur. Ct. H.R. ¶ 29 (1997); Case of Von Hannover v. Germany, Eur. Ct. H.R. ¶ 50 (2005).

174. Case of Krone Verlag GMBH & Co. KG v. Austria, Eur. Ct. H.R. ¶ 35 (2002).

175. *Id.* at ¶ 9.

Austria found the publication of the image unnecessary, preventing a newspaper from publishing it.[176] With respect to individual privacy, the ECtHR considers legitimate expectations. In *Von Hannover v. Germany*, the ECtHR reiterated that a person has a legitimate expectation of privacy in certain circumstances.[177] This court contended that although reporting facts can contribute to a public debate in a democratic society, the curiosity of a few people cannot count as a contribution to a public debate with general interest.[178] In his concurring opinion, Judge Cabral Barreto added that such circumstances cannot be determined concretely, unless courts apply a case-by-case approach to recognize whether a legitimate expectation exists.[179] For instance, in *Halford v. The United Kingdom,* the court held that telephone calls from business premises may fall into the notion of private life protected by Article 8.[180]

In *Hajovsky v. Slovakia*, given the fact that images indicate people's distinguishing characteristics, the ECtHR echoed that a person's image is an integral part of one's personality.[181] In this case, the applicant, a biological father, published an advertisement, seeking a woman who can give birth to his child.[182] Surrogacy was not recognized by Slovak law.[183] An investigative reporter pretended that she was a potential surrogate mother, secretly recording an interview with the applicant.[184] In 2005, the report, alongside the recorded video, were widely circulated without the applicant's consent.[185] The ECtHR contended that individuals not only have a right to protect their images but also a right to control the use of images.[186] Accordingly, the ECtHR was persuaded that although the report could be a point of general interest, the publication of the applicant's images did not contribute to the public debate.[187]

It seems that the EU tends to expand the concept of privacy to include OSIF, ensuring that the dissemination of such information is consistent with the balance between freedom of expression and the right to privacy.[188] In *Hajovsky v. Slovakia*, the ECtHR argued that public availability of information like images cannot be taken for granted and that privacy is a point of concern, particularly in cases

176. *Id.* at ¶ 17.
177. *See* Case of Von Hannover v. Germany, Eur. Ct. H.R. ¶ 50 (2005).
178. *Id.* at ¶ 65.
179. *Id.* at ¶ 2.
180. Case of Halford v. The United Kingdom, Eur. Ct. H.R. ¶ 44 (1997).
181. Case of Hajovsky v. Slovakia, Eur. Ct. H.R. ¶ 29 (2021).
182. *Id.* at ¶¶ 5–6.
183. *Id.*
184. *Id.* at ¶ 5.
185. *See id.* at ¶¶ 5–6.
186. *See id.* at ¶ 29.
187. *Id.* at ¶ 45.
188. *Id.* at ¶ 48.

where a person neither reveals nor consents to its revelation.[189] In *Peck v. the United Kingdom*, the ECtHR emphasized that in some circumstances, like suicide attempts in public, the disclosure of the CCTV footage without blurring a person's face or getting one's consent is an attack on the right to privacy.[190]

The ECtHR recognized that the context of the disclosures might require particular scrutiny about one's right to privacy.[191] Further, the ECtHR contended that following the revelation, the victim's exposure to media to explain the facts related to the footage does not eliminate the victim's claim of privacy breaches.[192] In a nutshell, if open-source investigators aim to extract information from satellite images, they need to make sure that the publication does not contain identifiable information like people's faces. In this regard, taking photos in public places is one of the conditions considered by the EU.[193] Accordingly, the way and the extent to which data is used are other pivotal elements.[194] If identifiable information is a crucial factor to the report or the content, it should align with a debate of general interest. Notwithstanding this, satellite operators and non-state, open-source investigators must comply with the EU General Data Protection Regulation (GDPR) to secure data.[195]

2. GDPR as a Shield from Policy Breaches

In 2021, the EU established the European Union Agency for the Space Programme to foster competitiveness in the space industry and supply free and open access to space data.[196] The program comprises various components including Galileo, Copernicus, and GOVSATCOM.[197] Made up of multiple satellites, Copernicus is an EO

189. *Id.*

190. Peck v. The United Kingdom, Eur. Ct. H.R. ¶¶ 76–87 (2003).

191. *Id.* at ¶ 85.

192. *Id.* at ¶ 86.

193. *See* Caoilfhionn Gallagher, *CCTV and Human Rights: The Fish and the Bicycle? An Examination of Peck V. United Kingdom* 2 SURVEILLANCE & SOC'Y 270, 274–76 (2004).

194. *See id.*

195. Regulation 2021/696 of the European Parliament and of the Council of 28 April 2021 Establishing the Union Space Programme and the European Union Agency for the Space Programme and Repealing Regulations (EU) No 912/2010, (EU) No 1285/2013 and (EU) No 377/2014 and Decision No 541/2014/EU, 2021 O.J. (L 170/69) art. 104(1).

196. *Id.* at arts. 1, 3, 4.

197. *Id.* at art. 3(1)(a) ("[A]n autonomous civil global navigation satellite system (GNSS) under civil control, which consists of a constellation of satellites, centres and a global network of stations on the ground, offering positioning, navigation and timing services and integrating the needs and requirements of security.").

system that provides free geoinformation data and services.[198] Unlike Copernicus, GOVSATCOM is a security-based satellite constellation, assisting the EU with crisis management, natural disasters, and diverse surveillance like illegal trafficking.[199] Article 104(1) of Regulation 2021/696 points out that personal data associated with this program must conform to applicable laws on personal data protection, in particular, Regulations (EU) 2016/679 (GDPR) and (EU) 2018/1725 of the European Parliament and of the Council.[200]

Article 4(1) of the GDPR differentiates an identifiable from an unidentifiable person, stipulating that "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier."[201] Article 4(1) of the GDPR also specifies instances of an identifier, including "a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[202] An identifiable or identified natural person is now entitled to personal data that can be any information relating to this person.[203]

When personal data is processed, it falls into the GDPR's requirements.[204] In the case of satellite imagery, an open-source investigator might obtain, retain, disclose, or disseminate satellite images.[205] The satellite operator collects, records, structures, and retains images and gives access to them. All these activities severally are considered data processing.[206] Hence, non-state, open-source investigators, as well as satellite operators, must comply with the GDPR, provided that personal data belongs to EU residents and citizens. Plainly speaking, the GDPR applies to all entities, geographically located in the EU and out of the EU—an extraterritorial impact—[207] that target or collect data related to natural persons,

198. *Id.* at art. 3(1)(c).
199. *Id.* at princ. 100.
200. *Id.* at art. 104(1).
201. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regards to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1) art. 4(1).
202. *Id.*
203. *Id.*
204. *See id.* at art. 4(2).
205. *See id.* at princ. 158.
206. *See id.* at art. 4(2).
207. *See id.* at art. 3.1 (stipulating "[t]his Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.").

citizens, and residents of the EU, with the primary feature of the regulation being high monetary penalties for violations.[208]

Based on the current capabilities, satellite imagery cannot capture people's faces, but it provides images of one's house, car, and other types of belongings that might be used as OSIF to assist indirectly with identification.[209] Consistent with Opinion 4/2007 on the Concept of Personal Data, if these objects usually belong to someone, are under a person's influence, or contain geographical vicinity with that person, they can be considered as indirect information related to a person.[210] Subsequently, the advancement of satellite imagery coupled with high-resolution images falls into the concept of personal data, which should be protected under the GDPR.

Irrespective of high-resolution images, based on Article 4(1) of the GDPR, any information which can be helpful in identifying a natural person is personal data. This definition is loose enough to include objective and subjective information, opinions, or assessments.[211] Additionally, it entails that the source of information might be anything such as satellite imagery. Indeed, the pivotal factor is the relevance between a person and information; therefore, such information can be one's images, location, etc.[212] According to Article 5 of the GDPR, data processing must be consistent with lawfulness, fairness, and transparency for explicit and legitimate purposes.[213] Further, based on Article 5(1)(c), the GDPR promotes data minimization, limiting data collection to adequacy, relevance, and the purposes embedded in data processing.[214] The first requirement is the consent of the natural person whose personal data aims to be processed.[215] The necessity of data processing must align with a

---

208. *See id.* at art. 3.2 ("This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.").

209. *See* Santos & Rapp, *supra* note 80, at 285–86.

210. *See Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN WP 136, at 4 (June 20, 2007), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf [https://perma.cc/ZA3Q-NGVN] (archived Sept. 24, 2024).

211. *See* Santos & Rapp, *supra* note 80, at 283.

212. *See id.*

213. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regards to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1) art 5(1).

214. *Id.* at art. 5(1)(c).

215. *Id.* at art. 6(1)(a).

contractual relationship or a legal obligation.[216] Otherwise, processing can be deemed lawful if its performance contributes to the public or the legitimate interests.[217]

C. The United States

1. Constitutional Right to Privacy

Although there is no explicit reference to the right to privacy in the US Constitution, several amendments implicitly acknowledge various illustrations of this right.[218] For instance, the Fourth Amendment protects individuals from unreasonable searches and seizures that violate one's privacy.[219] In *United States v. Jones*, the United States Supreme Court held that the attachment of a Global Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment.[220] The Fourth Amendment requires state agencies to respect one's privacy during a search or aerial

216. *Id.* at arts. 6(1)(b)–(c).

217. *Id.* at arts. 6(1)(e)–(f).

218. *See* Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 745 (1989) (describing how the Supreme Court has stated a "right to privacy" might be discerned in the "penumbras" of various amendments) (citing Griswold v. Connecticut, 381 U.S. 479, 484).

219. *See* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

220. United States v. Jones 565 U.S. 400, 400 (2012).

surveillance.[221] In the case of non-state, open-source investigations, the First Amendment to the US Constitution is more relevant.[222]

The First Amendment is a pivotal factor in protecting freedom of expression.[223] However, the First Amendment does not support expressive conduct associated with unlawful activities. In *Branzburg v. Hayes*, the United States Supreme Court underscored that news agencies or reporters cannot justify criminal conduct, such as private wiretapping or stealing documents, even though it provides valuable information.[224] The Court held that "[t]he Amendment does not reach so far as to override the interest of the public in ensuring that neither reporter nor source is invading the rights of other citizens through reprehensible conduct forbidden to all other persons."[225] Regarding privacy concerns, claims backed by the First Amendment are sometimes restricted by privacy torts.[226]

In 1960, William Prosser specified four types of torts that constitute the law of privacy: intrusion upon solitude, public disclosure of private facts, publicity that places one in a false light, and appropriation of a person's name or likeness.[227] Among them, the intrusion and publicity of private facts are the most relevant to satellite imagery. The former aims to protect people's "right to control

---

221. Katz v. United States, 389 U.S. 347, 353 (1967). It should be noted that this case coined the reasonable expectations of privacy test in the United States. Although the US Supreme Court has yet to consider its applicability to aerial surveillance, numerous lower courts have found this test relevant to aerial surveillance. For instance, in Long Lake Township v. Maxon, the State of Michigan Court of Appeals held that "[t]he Fourth Amendment requires persons both to establish a legitimate expectation of privacy and to establish that society is prepared to recognize that expectation as reasonable." Lake Township v. Maxon, (Mich Ct App, No. 349230, March 18, 2021). Thus, the court concluded that "drone surveillance of this nature intrudes into persons' reasonable expectations of privacy, so such surveillance implicates the Fourth Amendment and is illegal without a warrant or a traditional exception to the warrant requirement:" Lake Township v. Maxon, (Mich Ct App, No. 349230, March 18, 2021). Further, in United States v. Jones, the US Supreme Court used the physical intrusion of property but highlighted that the reasonable expectation of privacy test was not supplanted the common law trespassory test but it had a supplementary nature: United States v. Jones 565 U.S. 400, 409 (2012).

222. *See* U.S. CONST. amend. I. ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.").

223. *See* Matin Pedram, Jean-Christophe Roberge, & Eugenia Georgiades, *Loose Lips and Internet Censorship: Freedom of Expression in India and Malaysia* 58 U.S.F. L. REV. 432, 438 (2024) (describing how a recent executive orders limit data collection in surveillance activities).

224. Branzburg v. Hayes 408 U.S. 665, 691 (1972).

225. *Id.* at 691–92.

226. *See* William L Prosser, *Privacy*, 48 CAL. L. REV. 383, 407–10 (1960).

227. *Id.* at 389.

access to [their] immediate surroundings."[228] In *Nader v. General Motors Inc.*, the New York Court of Appeals held that the gathered information should have a confidential nature and subsequent actions to collect information; shadowing, wiretapping Nader's telephone, and eavedropping by electronic tools[229] are "unreasonably intrusive."[230] Confidentiality means that the information is not "available through normal inquiry or observation."[231] Thus, approaching Nader's acqintances to gather information that was already revealed by Nader does not amount to an invasion of privacy.[232] Accordingly, so long as there is no interference with freedom of movement, prying or collecting information is consistent with the common law.[233]

In other words, "the mere gathering of information about a particular individual" does not amount to intrusion unless actions such as unauthorized wiretapping or eavesdropping are involved.[234] Consequently, satellite imagery is not an intrusion *per se* because it is assumed that high-resolution images from residential areas, properties, and cars fall into the notion of OSIF, even in the absence of one's consent.[235] In *Cohen v. California*, the United States Supreme Court opined:

> [w]hile this Court has recognized that government may properly act in many situations to prohibit intrusion into the privacy of the home of unwelcome views and ideas which cannot be totally banned from the public dialogue, . . .we have at the same time consistently stressed that we are often *captives outside the sanctuary of the home and subject to objectionable speech*.[236]

Thus, if such images provide confidential information, like places that are not publicly visible in a house or their residents, it can be deemed intrusive. In this regard, the victim must prove that these images bring about emotional distress as well.[237]

Non-state investigators entitled to gather and use OSIF, might be exposed to public disclosure of private facts (PDPF). Indeed, the use of high-resolution images captured by satellites might be problematic on grounds of PDPF. Nobody can enjoy privacy in the public sphere—

---

228. *Privacy in the First Amendment*, 82 YALE L.J. 1462, 1473–74 (1973).
229. Kent Greenawalt, *New York's Right of Privacy – The Need for Change*, 42(2) BROOK. L. R. 159, 169 (1975).
230. Ralph Nader v. General Motors Corporation 25 N.Y.2d 560, 567 (N.Y. 1970).
231. *Id.* at 561.
232. Greenawalt, *supra* note 229, at 169.
233. Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 421 (1977).
234. *Id.*
235. *See* Craig, *supra* note 91, at 562.
236. Cohen v. California 403 U.S. 15, 21 (1971).
237. *See* Butler, *supra* note 103, at 1064.

places that are publicly accessible or visible by individuals.[238] In addition, voluntarily disclosing private facts is inconsistent with secrecy; therefore, it is not possible to rely on this tort.[239] In *Cinel v. Connick*, the United States Court of Appeals for the Fifth Circuit posited that PDPF is not allowed unless "1) the defendant publicized information concerning the plaintiff's private life, 2) the publicized matter would be highly offensive to the reasonable person, and 3) the information is not of legitimate public concern."[240] Accordingly, nude pictures can be published so long as they are associated with a story that is of public interest.[241]

In *Shulman v. Group W Productions Inc.*, the Supreme Court of California considered newsworthiness, seeking to strike a balance between legitimate public interest and privacy.[242] The plaintiffs' car was overturned on a highway, and they were injured.[243] The cameraperson, who worked for a television producer, recorded the rescue mission.[244] The recorded video was edited and broadcasted on a documentary television show.[245] Plaintiffs argued that their privacy was violated and became publicly available.[246]

The Supreme Court of California mentioned "when a person is involuntarily involved in a newsworthy incident, not all aspects of the person's life, and not everything the person says or does, is thereby rendered newsworthy."[247] The court contended that the identification of the involved persons or the use of their images is an unnecessary invasion of privacy in the public sphere if such data does not add any significance to the story developed by news agencies.[248] Accordingly, newsworthiness is recognized "by assessing the logical relationship or nexus, or the lack thereof, between the events or activities that brought the person into the public eye and the particular facts disclosed."[249]

Open-source investigators might obtain high-resolution images from commercial satellite operators in the legitimate market. In this case, if such images end up identifying an individual's private matters,

---

238. Patricia Sanchez Abril, "*A Simple, Human Measure of Privacy*": *Public Disclosure of Private Facts in the World of Tiger Woods* 10 CONN. PUB. INT. L.J. 385, 390 (2011).

239. *See id*. at 391.

240. Cinel v. Connick 15 F.3d 1338, 1345 (5th Cir. 1994).

241. *See id*. at 1346.

242. *See* Shulman v. Group W. Productions, Inc., 18 Cal. 4th 200, 222–23 (1998).

243. *Id.*

244. *Id*. at 200–01.

245. *Id*. at 200.

246. *Id*. at 213.

247. *Id*. at 202.

248. *Id*. at 236–37.

249. *Id*. at 224.

which is not the subject of public interest, the First Amendment might be ceased. Imagine the investigator preparing a report of a drug dealer's business. The investigator might obtain satellite images to determine the targeted locations and customers. During this analysis, the drug dealer's place of domicile, the plate number, or the drug dealer's intimate relations might be identified, even though they have no newsworthiness. It seems that if the investigator publishes such information, PDPF might be triggered.

In addition, the government should restrict the constant dissemination of high-resolution images in order to prevent aerial surveillance conducted by non-state investigators. In the case of unlawful evidence, hypothesize that the investigator purchases high-resolution images from an illegitimate market like a provider who offers hacked data or an unlicensed foreign satellite operator beyond US jurisdiction. It is recommended that the First Amendment should not be invoked.[250] As an illustration, Section 1708.8 of the California Civil Code criminalizes constructive invasion of privacy via any kind of visual image that is deemed to be offensive to a reasonable person, provided that without using such a device, images could have been obtained only by a trespass.[251] An instance of privacy can be an engagement in "a private, personal, or familial activity."[252] Apart from this, the private sector can enforce self-regulatory measures to protect individual privacy. For instance, Albedo is the first company that can offer high-resolution imagery from space. This company emphasizes that "[w]e recognize the power of the very high-resolution imagery our system will collect. As a result, we will continue to work with recognized leaders in national security and privacy so that we will be both compliant with our legal responsibilities and responsive to ethical concerns regarding privacy."[253]

2. Data Protection Policies

It is a critical fact that new technologies, such as satellite imagery, are capable of gathering constant data about individuals, irrespective of their awareness. At this point, non-state investigators and state agencies can collect a vast amount of information.[254] Nevertheless, in 2023, the US government unveiled the United States Novel Space

250. *See* Kirby Shilling, *Bad Publicity: The Diminished Right of Privacy in the Age of Social Media*, 32 FORDHAM INTELL. PROP., MEDIA, & ENT. L.J., 756, 800 (2022).

251. CAL. CIV. CODE § 1708.8 (2023).

252. *Id.* at § 1708.8(b).

253. *Albedo, supra* note 27.

254. Laura Hecht-Felella, *The Fourth Amendment in the Digital Age: How Carpenter Can Shape Privacy Protections for New Technologies*, BRENNAN CTR. FOR JUST. (Mar. 18, 2021), https://www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age [https://perma.cc/599F-X6AG] (archived Sept. 14, 2024).

Activities Authorization and Supervision Framework [255] that complemented the legislative proposal—the Authorization and Supervision of Novel Practice Sector Space Activities Act. This regulatory framework aims to address novel space activities that use emerging technologies and fall beyond the current regulatory regime.[256] Despite this, neither the framework nor the proposed act contains any reference to privacy concerns arising from commercial satellite imagery.[257] While the Fourth Amendment can be invoked to constrain the mass, warrantless surveillance conducted by state agencies, widespread access to satellite images might bedevil privacy breaches across the United States. Emerging technologies always pose challenges to the scope of the Fourth Amendment. As an illustration, in the United States, law enforcement used geofence warrants to force tech companies to determine who might be at a given location through their databases. [258] In this respect, in 2019, Google received approximately 180 geofence warrant requests from law enforcement on a weekly basis.[259] However, in *United States v. Smith*, the United States Court of Appeals for the Fifth Circuit held that "geofence warrants are modern-day general warrants and are unconstitutional under the Fourth Amendment."[260]

Further, different levels of access might be effective for the utilization of satellite images. To this end, satellite classification for licensing can be employed to restrict targeted groups from having access to ultra-high-resolution images. In 2020, the United States introduced three tiers with different regulatory conditions to categorize and license satellites based on each satellite's capability in producing unenhanced data.[261] Accordingly, based on Tier 1 of the categorization, "the bare minimum of conditions" is applied when the applicant can provide unenhanced data that is equivalent to the available data in the

---

255. *See* THE WHITE HOUSE, U.S. NOVEL SPACE ACTIVITIES AUTHORIZATION AND SUPERVISION FRAMEWORK 3 (2023).

256. Clayton Swope, *Mission Authorization: Decoding the Space Policy Dilemma*, CTR. FOR STRATEGIC & INT'L STUD. (Dec. 20, 2023), https://www.csis.org/analysis/mission-authorization-decoding-space-policy-dilemma [https://perma.cc/Y3JA-8GMV] (archived Sept. 14, 2024).

257. *See generally* THE WHITE HOUSE, U.S. NOVEL SPACE ACTIVITIES AUTHORIZATION AND SUPERVISION FRAMEWORK, *supra* note 255; Authorization and Supervision of Novel Private Sector Space Activities Act Draft Bill Text (2023), https://www.whitehouse.gov/wp-content/uploads/2023/11/Authorization-and-Supervision-of-Novel-Private-Sector-Space-Activities_Legislative-Text_final.pdf [https://perma.cc/UXZ2-ZF9C] (archived Oct. 11, 2024).

258. United States v. Smith, 110 F.4th 817, 838 (5th Cir. 2024).

259. *Id.*

260. *Id.*

261. License of Private Remote Sensing Space Systems, 85 Fed. Reg. 30790 (May 20, 2020) (to be codified at 15 C.F.R. pt. 960)

global market.[262] Tier 2 represents the situation in which the proposed system is the same as US sources; therefore, stricter regulations can be effective because there are no non-US sources to outcompete the US satellite operators.[263] Tier 3 is associated with completely novel systems with outstanding capabilities that do not exist in the United States or foreign markets.[264] In this case, in addition to Tier 2 requirements, there might be temporary restrictions on the dissemination of data to ensure that the US government can reduce any harm resulting from emerging capabilities.[265] In July 2023, a large part of these restrictions was lifted, and the remaining part related to national security must be validated by the Department of Defense each year.[266]

Satellites that fall into Tier 2 or 3 may need to employ cybersecurity measures to ensure "[p]ositive spacecraft control, [s]uccessful implementation of limited-operations directives, and [a]ddressing other national security concerns or international obligations and policies based on the unique capabilities of the system."[267] However, it is believed that privacy concerns are not addressed[268] by the Rule on Licensing of Private Remote Sensing Space Systems 2020.[269] Given the fact that ultra-high-resolution images may be licensed based on Tier 3 requirements, it is more likely that the sales

---

262. *Id.* at 30790, 30792. Based on PDD-23, in consultation with DoD, the Department of Commerce is authorized to restrict data collection and distribution via remote sensing space systems (i.e., shutter control). However, as global competition in satellite imagery is at its height, the U.S. government excludes licensees fall into Tier 1. *Id.* PDD 23 stipulates that "[d]uring periods when national security or international obligations and/or foreign policies may be compromised, as defined by the Secretary of Defense or the Secretary of State, respectively, the Secretary of Commerce may, after consultation with the appropriate agency(ies), require the licensee to limit data collection and/or distribution by the system to the extent necessitated by the given situation. Decisions to impose such limits only will be made by the Secretary of Commerce in consultation with the Secretary of Defense or the Secretary of State, as appropriate." Presidential Decision Directive/NSC-23 3–4 (March 9, 1994), https://irp.fas.org/offdocs/pdd/pdd-23.pdf [https://perma.cc/ECZ7-XFTU] (archived Oct. 11, 2024).

263. Licensing of Private Remote Sensing Space Systems, 85 Fed. Reg. 30790, 30792 (May 20, 2020).

264. *Id.*

265. *Id.*

266. *NOAA Eliminates Restrictive Operating Conditions From Commercial Remote Sensing Satellite Licenses*, OFF. SPACE COM. (Aug. 7, 2023), https://www.space.commerce.gov/noaa-eliminates-restrictive-operating-conditions-from-commercial-remote-sensing-satellite-licenses/ [https://perma.cc/6D9H-GKLE] (archived Sept. 14, 2024).

267. NAT'L OCEANIC & ATMOSPHERIC ADMIN., NO. 960.9(A)-1, POLICY GUIDANCE: CYBERSECURITY MEASURES (2022).

268. Licensing of Private Remote Sensing Space Systems, 85 Fed. Reg. 30790, 30792 (May 20, 2020).

269. 15 C.F.R. § 960 (2020).

of such images are limited to the government with stricter legal constraints originating from the Fourth Amendment.

Consistent with this view, almost eighteen states have enacted laws requiring law enforcement agencies to obtain warrants before surveillance.[270] Illinois' Freedom from Drone Surveillance Act bans a law enforcement agency from using onboard facial recognition software or using the gathered information with any facial recognition software.[271] In addition, based on 42 U.S.C. § 1983, any person who is under color of any statute that deprives someone of any constitutional or statutory right must be liable to the injured party;[272] therefore, in the case of abusive surveillance, the victim, whose privacy is violated, can bring the agency to trial. Further, ultra-high-resolution images can follow the identical classification for the information collected by drones. In 2015, a Presidential Memorandum stipulated that state agencies using unarmed aerial surveillance (UAS) must collect information that is completely linked to an authorized purpose and should not keep the UAS-collected information for more than 180 days unless a longer period is required by other applicable laws.[273] Such agencies are not allowed to disseminate the UAS-collected information unless it is required by law or justified by an authorized purpose.[274]

It should be noted that the application of property rights to determine the extent of one's private property and aerial trespass seem to be straightforward and simple.[275] Hence, any surveillance or imaging conducted by state agencies out of the determined area does not amount to a privacy breach.[276] Nevertheless, it cannot be a viable option for satellite imagery because there is no opportunity to recognize whether a person is being watched because of distance.[277] In order to find out the complexity of satellite imagery, it is more effective to rely on the majority's approach in *Carpenter v. United States*. In this case, the United States Supreme Court echoed that the central purpose of the Fourth Amendment is to shield individuals' privacy and security

---

270. Lexipol Content Development Team, *Key Considerations for a Law Enforcement Drone Policy*, POLICE1 (Mar. 11, 2024), https://www.police1.com/police-products/Police-Drones/key-considerations-for-a-law-enforcement-drone-policy [https://perma.cc/32R3-A448] (archived Sept. 29, 2024).

271. 725 ILL. COMP. STAT. 167/17 (2024).

272. 42 U.S.C. § 1983 (1996).

273. Memorandum on Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, 80 Fed. Reg. 9355 (Feb. 15, 2015).

274. *Id.*

275. Randall Khalil, *Aerial Trespass and the Fourth Amendment,* 121 MICH. L. REV. 1269, 1298 (2023).

276. *Id.*

277. Steele, *supra* note 63, at 328.

from arbitrary invasions conducted by governmental officials.[278] The United States Supreme Court considered convenience, affordability, and efficiency, which make new technologies more pervasive.[279]

Additionally, the Court opined that technologies such as drones, GPS, and cell phone location information are difficult to regard as voluntary because such technologies are "about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[280] The Court also acknowledged that individuals can reasonably expect privacy "in the whole of their physical movements."[281] In like fashion, in *United States v. Jones*, the United States Supreme Court reiterated that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[282] In this respect, the United States Supreme Court considered the cost of surveillance as a criterion to determine whether new surveillance technologies require a warrant.[283] In addition, the Court posited that GPS information can be an "intimate window into a person's life" by tracking one's movements, which in turn reveals a person's "familial, political, professional, religious, and sexual associations."[284]

V. CONCLUSION

With broader technological developments, satellite imagery may be capable of capturing high-resolution images from individuals across the world. This makes satellite imagery an industrial behemoth. Satellite imagery can be used by governments to strengthen national security, control adversaries, evaluate natural disasters, and improve law enforcement processes. Further, it can contribute to independent investigations led by individuals or non-state institutions. Hence, satellite images can count as a valuable source of OSIF that contribute to the decentralization of investigations. Nevertheless, satellite imagery can bring about privacy concerns where individuals are identifiable through images. Satellites are not only invisible but also can reach places that other technologies, such as facial recognition, cannot.

Although the limited market made up of a few satellite operators can be largely managed by implementing legal constraints, the proliferation of satellite imagery and the growing market of images

278. Carpenter v. United States, 585 U.S. 296, 303 (2018).
279. *Id.* at 311.
280. *Id.* at 315.
281. *Id.* at 310.
282. United States v. Jones 565 U.S. 400, 430 (2012).
283. Carpenter, 585 U.S. at 310.
284. *Id.* at 311.

make it difficult for governments to determine effectively the quality of images and set comprehensive privacy requirements. This Article addresses the privacy laws and policies in Australia, the EU, and the United States. It is acknowledged that the commercialization of satellite imagery and accessibility of high-resolution images may challenge the balance between freedom of expression and privacy in these countries. At this point, these legal systems are urged to put into practice progressive interpretations that favor new technologies but embrace lawsuits on grounds of privacy breaches in places with reasonable expectations of privacy.

Additionally, Australia and the EU enforce data protection policies that require satellite operators to minimize the collection and dissemination of personal information of an identified person. By contrast, the United States has yet to implement a comprehensive data protection policy, even though the right to privacy is recognized by the First Amendment. Despite this, the new licensing regime can be helpful in restricting the availability of high-resolution images in the market. Further, a reasonable expectation of privacy, as well as the risk of PDPF, can limit the publication of unnecessary information embedded in satellite images. These legal safeguards can promote commercial satellite imagery, encourage non-state, open-source investigations and undercut the dissemination of unnecessary information lacking any public interests.