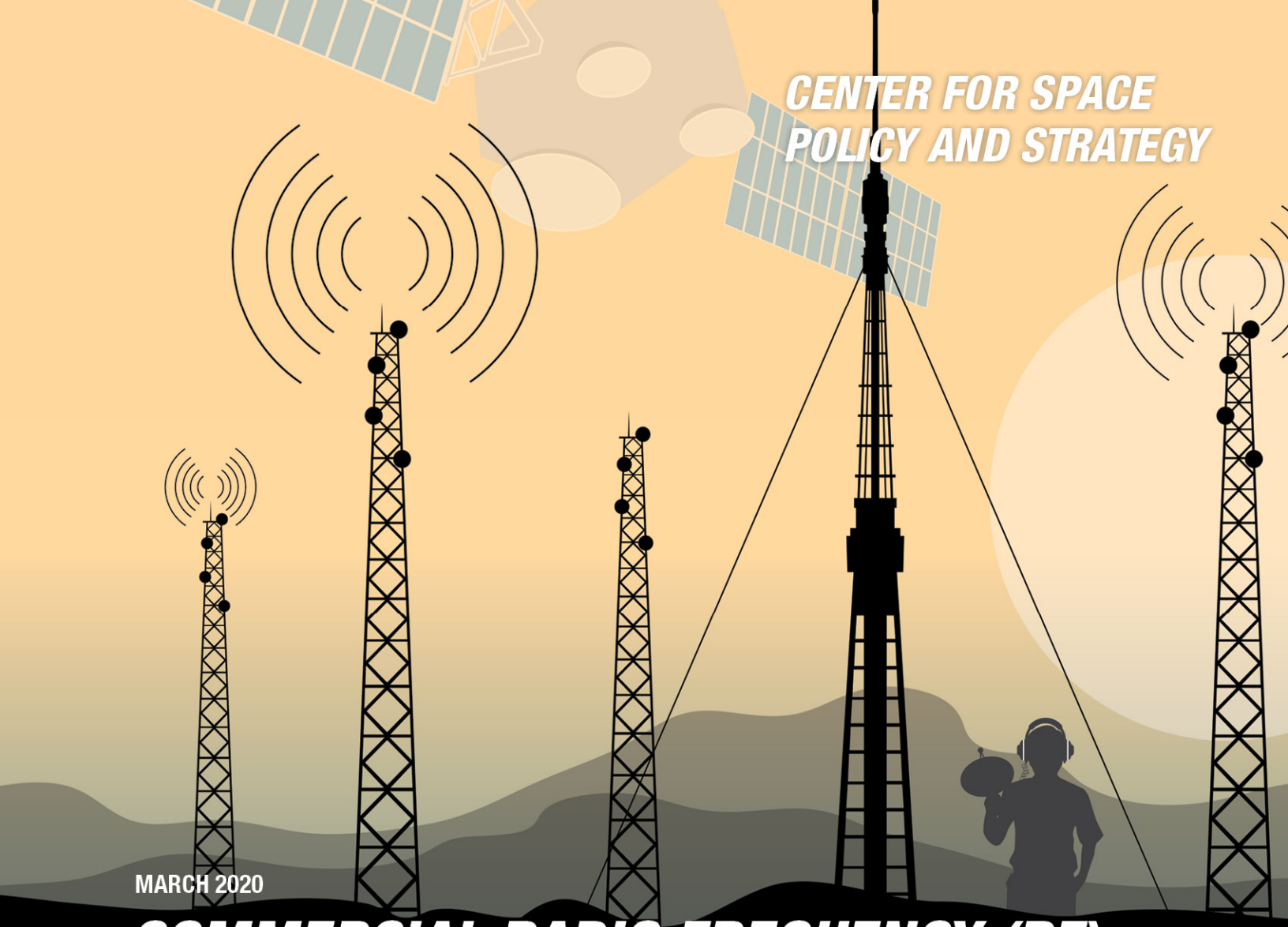

CENTER FOR SPACE POLICY AND STRATEGY

MARCH 2020

COMMERCIAL RADIO FREQUENCY (RF) COLLECTIONS FROM SPACE

JAMES A. VEDDA AND JOSEF S. KOLLER
THE AEROSPACE CORPORATION

AEROSPACE

DR. JAMES A. VEDDA

Dr. James A. Vedda is a senior policy analyst performing policy research and evaluation for various government agencies. He is the author of *Becoming Spacefarers: Rescuing America's Space Program and Choice, Not Fate: Shaping a Sustainable Future in the Space Age*. He holds a master's degree in science, technology, and public policy from George Washington University and a Ph.D. in political science from the University of Florida.

DR. JOSEF S. KOLLER

Dr. Josef S. Koller is a senior systems director for The Aerospace Corporation's Center for Space Policy and Strategy, serving as an analyst and team leader on topics that cut across policy, technology, and economics. Prior to joining Aerospace, Koller served as a Senior Advisor to the Office of the Secretary of Defense for Space Policy, where he directly supported key national and international strategy efforts and provided technical advice and analysis on space-related U.S. government and DOD policy matters, including commercial remote sensing and space traffic management policy matters. Prior to that assignment, Koller managed and co-led over 40 scientists in the "Space Science and Applications Group" at Los Alamos National Laboratory. Koller also established and led the Los Alamos Space Weather Summer School to promote graduate student research. Koller has over 17 years of experience with global security and space physics programs. He has authored over 50 peer-reviewed scientific publications with 700+ citations. Koller has a Ph.D. in astrophysics from Rice University as well as master's degrees in physics and astronomy from the University of Innsbruck, Austria.

ABOUT THE CENTER FOR SPACE POLICY AND STRATEGY

The Center for Space Policy and Strategy is dedicated to shaping the future by providing nonpartisan research and strategic analysis to decisionmakers. The center is part of The Aerospace Corporation, a nonprofit organization that advises the government on complex space enterprise and systems engineering problems.

Contact us at www.aerospace.org/policy or policy@aero.org

Summary

Commercial radio frequency (RF) collection services are entering the space sector with the capability to detect and geolocate a range of RF signals from emitters of interest. This paper examines current and future operators and their RF services for both governmental and nongovernmental customers. Based on current U.S. policy, law, and interviews with U.S. government stakeholders, it also examines how this new capability fits into the commercial space regulatory framework given the current and historical legal context in the United States and abroad. Options are presented here for specific actions to strengthen national security, foreign policy, and individual privacy protections with the advent of commercial RF collection.

An Emerging Policy and Regulatory Issue

Technological advances and their rapid diffusion can create challenges for U.S. law, policy, and regulation. New or improved information collection technologies present both opportunities and concerns for national security, foreign policy, privacy, and the safekeeping of proprietary information.

Space-based commercial RF collection systems are designed to detect and geolocate a range of RF signals from emitters of interest, such as handheld very high frequency (VHF) radios, maritime radar systems, automated information system (AIS) beacons, very small aperture terminals (VSATs), and emergency beacons. The detected signals can also be processed and analyzed to produce useful information about spectrum use in a particular region or about the emitters themselves. Emerging commercial operators believe there is a market for the information they produce among governments, industry users, and nonprofits. Although their stated aim is not to intercept and examine the content of message traffic, the potential for such operations raises concerns in national security circles because these services represent the first wave of nongovernment entities conducting such collections from space.

Commercial RF collection has the potential to augment U.S. government (USG) signal monitoring capabilities by providing a complementary data source that can be shared in unclassified channels with international allies, state and local governments, law enforcement, and first responders. Its widespread availability also brings risks. Passive collection of electromagnetic signals is difficult to police as it only requires a receiver tuned into the frequency of emissions. Efforts to restrict collection in certain frequencies or specific geographic areas may prove ineffective or even counterproductive if

they lead to the identification of sensitive areas, frequency bands, or operations. Like commercial satellite imagery collection, which prompted efforts to exclude certain geographic targets from public availability, attempts to protect specific sensitive frequencies could result in restricted access to large sections of spectrum, a potentially serious impediment to the nascent commercial signals collection market.

There are no laws, policies, or regulations that specifically prohibit or enable RF collection from space by a U.S. private entity. RF collection does not fit into accepted definitions of remote sensing, which are focused on imagery derived from reflected or emitted electromagnetic waves. Because commercial RF collection is a relatively new capability, U.S. policies and laws governing space-based RF collection activity only address collection by government agencies. Their applicability to emerging commercial RF collection businesses and the regulatory authority of agencies is unclear because existing guidance was not designed to cover private-sector activity.

Research and stakeholder interviews conducted by the authors indicate that current remote sensing policies, laws, and regulations are inadequate for proper oversight of commercial RF collection, but other statutory aspects are in place that can be used as a foundation. In general, there is no consensus on a specific path to resolve the situation. To achieve consensus, we suggest the following objectives while shaping a U.S. legal and regulatory regime:

- Fulfill the international requirement in the Outer Space Treaty of 1967 to oversee all space activities of U.S. entities.
- Encourage U.S. commercial activity and a level playing field on the global market.
- Minimize the regulatory burden on U.S. industry to prevent unnecessary costs and delays.
- Ensure that U.S. commercial RF collectors comply with U.S. laws on privacy and national security.
- Explore the utility of commercial satellite RF products and services to augment USG missions.
- Guard against the use of domestic RF products and services in ways contrary to U.S. national security and foreign policy interests.

For decades, the USG operated on the assumption that RF collection from space was a government-only activity. That assumption is no longer valid. Given that commercial RF collections from space are well underway today, the time for deliberate actions to accomplish U.S. goals regarding such commercial activities has arrived. This paper suggests a variety of actions the USG could take and discusses the pros and cons of each. These actions are not mutually exclusive, and not all of them may be required.

Commercial Capabilities

Existing and prospective commercial providers believe there is a market for space-based RF collection services that includes industry customers and government agencies around the world. Proposed product offerings include:[1]

- Aerial, terrestrial, and maritime transportation tracking.
- Emergency response, including search-and-rescue efforts.
- Communications interference detection and geolocation.
- Spectrum mapping to increase efficiency and support decisionmaking.
- Space situational awareness (SSA).

Transportation, Tracking, and Maritime Awareness

RF collection is demonstrating the potential to bring greater value to this market through its geolocation services and ability to collect from a broader spectrum of signals, like space-based AIS, which have a current market in ship tracking through the detection of required identification signals. RF collection would allow the ability to locate vessels in the sky, on land, and at sea. For example, HawkEye 360's geolocation model can provide location, speed, and course detection information that could help manage the legal fishing, shipping, and transportation industries.[2] Additionally, RF geolocation services are offering the capability to locate illegal activity and vessels that attempt to hide their actual location.

Automatic Identification System (AIS) Signals Collection

AIS signals collection is a subset of the RF data collected by commercial RF collection services. AIS is a method of attaching a radio tracking signature to transponders on ships to identify and locate ships. It integrates a very high frequency (VHF) transceiver with position-based satellite systems such as the global positioning system (GPS). In 2002, the International Maritime Organization (IMO), under the International Convention for the Safety of Life at Sea (SOLAS),[3] established the first set the standards that require ships to have AIS transceivers aboard ships. This allowed for maritime monitoring to be done on land or aboard vessels.

In 2008, the landscape for maritime monitoring changed with the rise of satellite-based AIS collection. Canadian company exactEarth was one of the first,[4] followed by U.S. companies such as Orbcomm, SpaceQuest, and Spire. These companies have focused their business models on selling data products and analytics in maritime awareness, asset tracking, and search-and-rescue using AIS signals collection.

New companies conducting RF geolocation differ from AIS signals collection companies in their technical capabilities. For example, HawkEye 360 can collect RF signals from a broad range of channels in addition to AIS transceivers.[5] Traditional AIS signals collection has been criticized for its lack of accuracy and reliability, inability to handle high levels of maritime signals traffic, and difficulty tracking illicit maritime activity. However, HawkEye claims that it will be able to pinpoint ships that are spoofing AIS signatures by changing their identifiers, replicating signatures to falsify location, or turning off receivers and going off the grid.

Emergency Response

RF collection has the potential to bolster emergency response by identifying and locating emergency beacons where a GPS receiver may be damaged or where poor GPS reception exists. While emergency response exists in many forms, search-and-rescue efforts have relied on satellites for decades. In an emergency, RF collection may help determine which communication signals are still working and which are not.

Communications Interference Detection

This application can allow RF collectors to monitor communication channels and provide data on any interference or anomalies to signal operators within those channels. RF collectors could detect, characterize, and locate the sources of interference. Though ground-based RF collectors offer this service, their scope and reach are limited. Space-based RF collectors have the potential to extend this application while remaining cost-competitive with ground-based services.

Spectrum Mapping

Providing data on RF spectrum usage over large regions may be the application that demonstrates the greatest advantage that space-based collection has over ground-based collection. In contrast to the limited coverage of ground-based initiatives, RF collection satellites theoretically could collect RF signal data over hundreds of miles.[6] Because parts of the electromagnetic spectrum are becoming congested, the ability to characterize its use in near realtime and input the data into a visualization model could support spectrum allocation and use management.

Space Situational Awareness

RF data can be used to determine information about satellites such as location, health, performance, and behavior attribution. Kratos, a ground-based RF collector, offers SSA services, including satellite surveillance, correlative/predictive analytics, bandwidth utilizations, and interference mitigation services. Space-based RF collectors potentially could expand on these applications, providing tools with broader coverage to address increasing congestion in space. Kratos is already advertising space RF collection as a complementary phenomenology for spacecraft tracking and characterization.[7]

Existing and Planned Space-Based RF Collectors

Terrestrial commercial RF collectors have existed for quite some time. Companies offer worldwide antenna-based RF collection solutions and provide government and commercial satellite operators with carrier monitoring, interference detection, and geolocation services. Other companies like CRFS have been providing portable analyzers as a terrestrial-based solution since 2007.[8]

With the launch of HawkEye 360's first three satellites in December 2018, and with other companies to follow, a market is soon to open for space-based RF collection focused on offering geolocation services with broader and more comprehensive range of applications. The following paragraphs and Table 1 describe the most prominent space-based RF collection service providers that have launched or plan to launch soon to low Earth orbit.

HawkEye 360 (HE360) is a U.S.-based company with headquarters in Herndon, Virginia, that plans to launch a constellation of 18 to 36 satellites in clusters of three. Referred to as the *Pathfinder constellation*, this mission launched its first cluster on December 3, 2018.[9] The constellation will collect RF data from emitters such as handheld very high frequency (VHF) radios, maritime radar systems, AIS beacons, very small aperture terminals (VSATs), and emergency beacons, and triangulate and process the signals for more precise and accurate geolocation. The aim is to create an RF data layer for the entire planet that can be used to manage spectrum use; detect aerial, land, and sea vessels; and locate and characterize interference.

HE360 has partnered with a number of companies to provide RF data products, such as electro-optical (EO) operator BlackSky, ground-based RF collector Kratos,[10] and synthetic aperture radar (SAR) operator Ursa Space Systems.[11] HE360 aims to offer comprehensive data analytics that combine its RF data with other companies' EO and SAR data. It also has an agreement to supply data to Israel-based maritime risk analysis contractor Windward.[12] In direct services to the USG, HE360 has assisted the Department of Homeland Security (DHS) on a test and evaluation project to receive alerts from emergency beacons. During this test, emergency beacon alert data was detected and demodulated, retrieving GPS information but no data that would infringe on privacy rights.

In April 2019, HE360 began to market its first RF analytics product, called RFGeo[13], which provides signal coordinates from a broad range of RF emissions to create a map that includes location data and its associated location error data. This product is intended to complement other data sources for defense, border security, maritime monitoring, telecommunications, and emergency response applications.

Aurora Insight, a U.S.-based company in the Washington, D.C. area, launched an experimental payload called THEA on a SpaceQuest 3U CubeSat.[14] According to its website, the company is developing a "globally distributed network of specialized radio frequency sensors."[15] The

Table 1: Near-Term Satellite RF Collection Operators						
Entity	**Location**	**No. of Satellites**	**Satellite Type**	**Manufacturer**	**Proposed Architecture**	**Status**
HawkEye 360	Herndon, Virginia, U.S.A.	3 in orbit, 18–36 planned	15 kg microsat	GOMSpace payload; Deep Space Industries/ UTIAS platform	Three-satellite clusters to determine position based on TDOA and FDOA	Active; next cluster expected in early 2020
Aurora Insight	Washington D.C., U.S.A.	1 in orbit, planned number unknown	3U CubeSat	SpaceQuest	Basic low-cost VHF receiver on CubeSat	Active; tech demonstration
Kleos Space	Luxembourg	28 planned	1–10 kg nanosat	GOMSpace	7 four-satellite clusters	Launches begin in 2020
unseenlabs	Rennes, France	1 in orbit, planned number unknown	6U CubeSat	GOMSpace; Nexeya	Three-satellite cluster	Active; tech demonstration
Technion	Haifa, Israel	3 planned	6U CubeSat	Technion	Three-satellite clusters to determine position based on TDOA and FDOA	2018 launch postponed

company's products are expected to combine ground-based spectrum analytics with aerial solutions; however, with the launch of THEA in December 2018, the company has now added space-based RF collection to its portfolio as well. The THEA mission has been designated as a technology demonstration to determine if a low-cost VHF radio receiver can function on a small CubeSat. SpaceQuest, also a U.S.-based company, has particular experience and interest in developing satellites and satellite components that gather AIS data and in offering analytics services.[16]

Kleos Space, which has a business plan similar to HE360, is headquartered in Luxembourg and has offices in the United States, United Kingdom (U.K.), and Australia. The Kleos Scouting Mission includes a 20-satellite constellation intended to geolocate radio transmissions from any target electronic signals and then perform analytics on the data to provide "activity-based intelligence" for the purposes of maritime security, search-and-rescue, communication interference, and asset tracking for a variety of defense, commercial, and humanitarian purposes.[17] Its satellites are built by Danish company GOMSpace, the same company that is working on HE360 payloads. Kleos satellites will be nanosatellites between 1 and 10 kilograms that "may be launched individually, or...multiple nano-satellites working together or in formation."[18] The first four of these nanosatellites are scheduled to be launched in March 2020, with a second cluster scheduled to launch in the fall. Kleos sells its data products at three levels of subscription from wholesale, unprocessed data to fully tailored analytics: Guardian RF, Guardian LOCATE, and Guardian UDT.[19]

unseenlabs is a startup company based in Rennes, France, that will be conducting RF geolocation for

maritime awareness, specifically looking to find illegal fishing and shipping activities that are not emitting AIS signals.[20] The company will also be conducting other forms of asset tracking. Its satellites are also being built by GOMSpace.[21] It is not clear how many satellites are planned, but the first, BRO-1, was launched by Rocket Lab on August 19, 2019.[22]

Technion at the Israel Institute of Technology is a university-based, student-led initiative in Haifa, Israel, and funded by Adelis Foundation. The group plans to develop a cluster of three satellites called Space Autonomous for Swarming and Geolocating Nanosatellites (SAMSON) that will provide RF geolocation. Each satellite will be a 6U CubeSat that will be used to test the technology for long-term autonomous cluster flights of a multi-satellite system and determine the position of a cooperative terrestrial emitter based on time difference of arrival (TDOA) and frequency difference of arrival (FDOA).[23] The aim seems to be an academic study rather than a specific business plan. The satellites were scheduled to launch by the end of 2018, but the launch has been postponed.[24]

In addition to the long-standing terrestrial-based solutions, and the emerging satellite-based solutions that conduct large-scale RF collection, great opportunity exists to explore aerial-based services for localized RF collection. CRFS[25] and Horizon Technologies[26] are examples of companies already in this market, with the latter soon to add satellite RF collection. It is also possible that high-altitude platforms (HAPs) could augment large-scale RF collection efforts in remote areas where the terrain or weather interferes with communication signals. These can provide more effective coverage on a temporary basis over a smaller area. For example, Northrop Grumman developed the RQ-4 Global Hawk to conduct radar, optical, infrared, and signals intelligence, and monitoring for the U.S Air Force.[27] Currently, there are several commercial HAP development initiatives underway in Europe, China, Russia, and the United States. It is possible that these initiatives could perform RF signals collection if desired.

Technical developments (e.g., smallsat design, computer hardware and software, and launch availability) have made satellite RF collection capability more accessible and affordable. Technical developments have also made it possible for aerial-based local RF collection to enter the commercial sector and augment terrestrial-based systems. If a reliable global market for RF products evolves, more operators, both U.S. and foreign, will emerge to address it. Lessons from history indicate that unduly burdensome restrictions on U.S. operators will not resolve concerns that the U.S. national security community may have about this development. As Table 1 shows, this is already an international playing field.

Risks and Benefits of Commercial RF Collection from Space

Concerns for the USG

As the space domain continues to evolve, the rapid advance of commercial remote sensing in terms of technical capability and global coverage is a key concern of the U.S. national security community due to increased transparency. The USG will soon be operating in an environment in which every emission, on Earth and in space, could be observed, analyzed, and reported to unknown consumers in near-real time. This includes reflected light in the visible spectrum, infrared energy, and emitted signals from transmitters.[28] A recent publication by the Center for Space Policy and Strategy highlights the combined effect of global remote sensing, analytics based on artificial intelligence, and the distribution of those analytics directly to consumers via constellations of communication satellites.[29]

More persistent, broader coverage of commercial RF collection has benefits but comes with potential risks. Even if it is licensed, the passive collection of

signals is very difficult to police because it only requires a receiver. Furthermore, efforts to restrict collection in certain frequencies or specific geographic areas may prove ineffective, or even counterproductive, if they result in drawing unwanted attention to sensitive areas, frequency bands, or operations.

Commercial satellite imagery and ground-based employment of information collection technologies over the years have taught us lessons applicable to commercial RF collection. At the macro level, security and foreign policy concerns arise whenever new or improved collection technologies emerge that are publicly available and are leveraged by foreign nations and non-state actors. Similarly, at the micro level, privacy and proprietary information may be at risk. The USG has initiated solutions through laws, policies, and judicial precedent. A similar pattern can be expected for RF collection, although it is important to recognize that the solutions of today are moving targets due to unceasing technological advances and their rapid diffusion. Judicial rulings illustrate this well. They hinge on evolving conditions such as expectations of privacy in particular situations and the level of technology available to the general public.[30,31,32,33] These conditions can change dramatically in just a few years.

Benefits to the USG. When the U.S. private sector becomes a routine provider of products or services traditionally employed exclusively by large nation-states, an opportunity exists to supplement existing capacity or replace it entirely, possibly saving tax dollars in the process. Existing space-related examples include satellite communications, overhead imaging, and cargo and crew delivery to low Earth orbit. The transition can be difficult, as it was for satellite imagery, which prompted serious questions for the U.S. national security community. How can unclassified but potentially sensitive data be protected in commercial data storage and sharing systems? How will commercial data purchases be handled in the budget? Can commercial providers be relied on for long-term production of timely, high-quality data given the ebb and flow of market forces? However, USG stakeholders, particularly the National Geospatial-Intelligence Agency (NGA) for satellite imagery, found ways to address these concerns.

As it was true for commercial imagery, commercial RF signal collection has the potential to contribute to USG efforts by providing a complementary data source that can be shared on unclassified channels with international allies, state and local governments, law enforcement, and first responders. It can offer more persistent, broader coverage than terrestrial offerings and could be focused on routine tasks to free up the USG's more capable assets for higher-priority targets. Like national collection systems, existing laws, regulations, and other guidance will apply to the USG use of electronic surveillance, especially as it concerns U.S. persons.

The Definition Problem

One suggested approach to the licensing, regulation, and USG use of commercial satellite RF products is to treat them as a subset of satellite remote sensing products. However, RF collection does not fit into accepted definitions of remote sensing, which are focused on imagery derived from reflected or emitted electromagnetic waves. RF collection is a form of electronic surveillance that traditionally has been a government activity, so policies and laws governing that activity have been aimed at the behavior of government agencies. The applicability of current laws to commercial RF collection, and the regulatory authority of agencies, are unclear because existing guidance was not designed to cover private-sector activity.

The Land Remote Sensing Policy Act of 1992 (LRSPA),[34] which was the first successful commercial remote sensing statute, is the starting point in a search for clarity. It provides the

Department of Commerce (DoC) with licensing and regulatory authority over *land remote sensing*, which is defined as

> …the collection of data which can be processed into imagery of surface features of the Earth from an unclassified satellite or satellites, other than an operational United States Government weather satellite.

RF collection does not produce imagery of surface features of the Earth, which would place it beyond the scope of this definition. Regarding the legislative intent behind the statutory language, the relevant House[35] and Senate[36] reports reveal that licensing of remote sensing systems was intended to be kept separate from licensing of radio frequency systems. Although Congress defined *land remote sensing* as the collection of imagery of the Earth's surface, when Congress created the authority for DoC to issue licenses, it did not limit this authority to land remote sensing. Instead, it provided DoC with a broader authority over all "private remote sensing space systems."[37] Subsequently, and based on the definitions provided by Congress, DoC's National Oceanic and Atmospheric Administration (NOAA) then defined *remote sensing space systems* as follows in the regulations:

> Any device, instrument, or combination thereof, the space-borne platform upon which it is carried, and any related facilities capable of actively or passively sensing the Earth's surface, including bodies of water, from space by making use of the properties of the electromagnetic waves emitted, reflected, or diffracted by the sensed objects.[38]

Again, since RF collection does not sense objects or the Earth's surface, it is not included in this definition. Even in cases in which a commercial satellite system performs remote sensing and serves other purposes, DoC licensing authority "shall be limited only to the remote-sensing operations of such a space system." Currently, DoC is rewriting its regulations, but the published proposed rule does not indicate a significant change in the definitions of *remote sensing* or *remote sensing space systems*. However, it is important to note that the proposed rule does not explicitly preclude DoC from exercising its authority to regulate RF sensing.[39]

Internationally, the widely accepted United Nations principles on remote sensing provide another definition for consideration:

> The term *remote sensing* means the sensing of the Earth's surface from space by making use of the properties of electromagnetic waves emitted, reflected or diffracted by the sensed objects, for the purpose of improving natural resources management, land use and the protection of the environment.[40]

This resembles the LRSPA definitions discussed above, specifying sensing of the Earth's surface and use for particular applications or characteristics not applicable to RF collection.

This discussion demonstrates that commercial remote sensing definitions taken from U.S. law, U.S. regulations, and international principles clearly do not apply to commercial RF collection.

Current U.S. Guidance Documents: Few Answers, Many Remaining Questions

In addition to the problem of defining the terms, there are no laws, policies, or regulations that specifically prohibit or enable RF collection from space by a U.S. private entity. The **National Space Policy (2010)**[41] opens the door for commercial RF collection without explicitly authorizing or facilitating such activities. It states that the USG shall:

> Enhance capabilities and techniques, *in cooperation with* civil, *commercial*, and foreign partners, to *identify, locate, and attribute sources of radio frequency interference*, and take necessary measures to sustain the radiofrequency environment in which critical U.S. space systems operate. [emphasis added]

This implies that the USG endorses commercial operations involving RF collection. Additionally, the policy directs the Secretary of Defense (SecDef) and the Director of National Intelligence (DNI) to:

> Improve, develop, and demonstrate, in cooperation with relevant departments and agencies and *commercial* and foreign entities, the *ability to rapidly detect, warn, characterize, and attribute natural and man-made disturbances to space systems* of U.S. interest. [emphasis added]

The DNI is also directed to:

> Coordinate on any radiofrequency surveys from space conducted by United States Government departments or agencies and *review, as appropriate, any radiofrequency surveys from space conducted by licensed private sector operators* or by state and local governments. [emphasis added]

This implies that the USG will license commercial operators, although such a licensing structure has not yet been established through a specific rulemaking. The National Space Policy does not define what it means by "radiofrequency surveys" or identify what type of collection and processing capabilities are permissible for commercial operators.

Federal statutes on *crimes and criminal procedures* address the interception of communications. Chapter 119 of Title 18, codifying the Electronic Communications Privacy Act of 1986 (the Wiretap Act), prohibits any person from intercepting and disclosing wire, oral, or electronic communications, declaring that no part of the contents of illegally obtained communications is admissible as evidence. However, it also enumerates a variety of interception means and circumstances that are not considered unlawful. For example, it is not considered unlawful to intercept transmissions from a communications medium that is readily accessible to the general public and carries no expectation of privacy, such as law enforcement and safety systems, citizens band radio, or other mobile radio services. Regarding the services offered by commercial RF collectors, it is also permissible to intercept any electronic communication that is produced by any marine or aeronautical communications system; or causing harmful interference, to the extent necessary to identify its source.[42]

The same prohibitions against interception and disclosure can be found in Title 47 (Telecommunications), which refers back to Title 18 and its exemptions.[43]

The **Foreign Intelligence Surveillance Act** (FISA)[44] of 1978 addresses electronic surveillance.[45] FISA is designed to protect U.S. persons from inappropriate surveillance by the USG and to prevent unnecessary retention and dissemination of information on U.S. persons. FISA defines "minimization procedures" that are to be specified in agency plans and approved by the U.S. attorney general. These are specific procedures to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning U.S. persons who have not given their consent. Exceptions can be made for information that is evidence of a crime that is being used for law enforcement purposes and for information necessary to understand foreign intelligence or assess its importance.

While FISA does not specifically address electronic surveillance carried out by the U.S. private sector, it is clear that if USG agencies were to incorporate commercial RF collections into their surveillance efforts, they would still need to follow FISA's rules on protection of U.S. persons when using the commercial product. This could prove difficult if satellite RF collectors sweep up signals from a large geographic area or from ships with U.S. persons on board, for example. In general, however, relevant guidance leaves the door open for USG use of commercial RF products and services.

The **USA PATRIOT ACT of 2001**[46] serves as a counterbalance to the FISA in granting increased powers of surveillance to national security and intelligence communities. Title II, "Enhanced Surveillance Procedures," specifically grants the authority to intercept wire, oral, and electronic communications aiding and relating to criminal investigations in crimes such as terrorism and computer fraud. The act authorizes disclosure of such "foreign intelligence information" to national law enforcement authorities; presumably such information can be disclosed by private entities, but there is no clear demarcation of who can disclose such information, only to whom they may make such disclosures.

Other relevant guidance can be found in executive branch documents such as the following:

- **Executive Order (EO) 12333**[47] on intelligence activities states that "agencies within the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States." The agencies are permitted to collect, retain, and disseminate "information that is publicly available," which may include information that is available for sale on the open market.

- **DOD Directive 5100.20** serves as the charter for the National Security Agency (NSA), the sole agency authorized to routinely engage in signal intelligence (SIGINT) activities.[48] Accompanied by a supporting instruction,[49] DoDD 5100.20 gives the director of NSA the responsibility to "collect (including through clandestine means), process, analyze, produce, and disseminate SIGINT information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions." The parenthetical inclusion of "clandestine means" implies that NSA may collect by other means, including the purchase of commercial products. Additionally, the director must establish policies and procedures to ensure that the SIGINT mission is "accomplished in the most efficient and effective manner," which could be viewed as an opening for the use of commercial sources.

- Intelligence directive **USSID SP0018**[50] provides implementation procedures for many of the policies listed in the FISA, EO 12333, and related DOD directives. Like EO 12333, there are exceptions to allow collection of distress signals, illicit activities, and transmitter locations outside of the United States.

- The DoC's **Bureau of Industry and Security (BIS)**[51] is the primary office for setting guidelines for conducting business and trade with an eye toward national security concerns. It manages restrictions on exports by U.S. companies through the Denied Persons List, Entity List, Unverified List, and Consolidated Screening List. For example, U.S. RF collection companies would not be able to sell data or conduct any transaction with anyone on the Denied Persons List. Technologies subject to the Export Administration Regulations (EAR), such as HawkEye 360's software for RF collections, cannot be sold to anyone on the Entities List.

Potential Actions in U.S. Policy, Law, and Regulation

HawkEye 360 and Aurora Insight have begun deploying their satellites with other domestic and international operators to follow. From our interviews, we detected a sense of urgency among USG stakeholders to establish consensus on oversight and regulation of this emerging capability, followed by an effort to promote the U.S. approach internationally, thereby establishing norms of behavior. Other spacefaring countries have looked to the United States for ideas on legal and regulatory regimes in other areas (such as commercial space launch), and the United States has had success in exporting its space-related best practices (such as in orbital debris mitigation). It may be possible to repeat this experience to establish best practices for commercial RF collection.

The authors found general agreement that current policy, law, and regulations are inadequate for proper oversight of this activity, but many aspects are in place that could be used as a foundation. However, there was no consensus on changes to legal definitions or any other specific path to resolve the situation.

To start the resolution process, the USG could consider setting the parameters for what a legal and regulatory regime is intended to accomplish. Our research and interviews suggest the following:

- Fulfill the international requirement to oversee the space activities of U.S. entities.
- Encourage U.S. commercial activity and a level playing field on the global market.
- Minimize the regulatory burden on U.S. industry to prevent unnecessary costs and delays.
- Ensure that U.S. commercial RF collectors comply with U.S. laws on privacy and national security.
- Explore the utility of commercial satellite RF products and services for USG missions.
- Guard against the use of domestic RF products and services in ways contrary to U.S. national security and foreign policy interests.

As in other areas of high-tech commerce, there is inherent tension between national security concerns and the desire for U.S. industry to achieve success, or even dominance, in the world market. In the case of satellite RF collection, this tension is heightened by the fact that, until recently, the activity has been conducted solely by government intelligence agencies. Relevant guidance reviewed for this study (statutes, executive orders, agency directives, etc.) did not envision commercial actors in this area and, therefore, offered no direction on licensing, regulatory, or security actions necessitated by the broad availability of RF collection services on the commercial market.

The actions to date of emerging U.S. RF collection operators have been conscientious about national security concerns, but similar behavior by other new entrants cannot be assumed. Safeguards may need to be put in place, but with care, since burdensome, retroactive regulation would be problematic, interfering with previously approved business plans and possibly prompting legal challenges.

An agency charged with oversight of commercial RF collection could employ and monitor safeguards without overburdening the fledgling U.S. industry. One USG official suggested that the agency responsible should, at a minimum, do two things:

1. Provide improved tools and resources for USG agencies to monitor market activity and anticipate market evolution.
2. Establish access to a critical mass of expertise to support government officials with approval authority. This would improve efficiency and

prevent prolonged deliberations that could drive firms overseas or exhaust funds/resources before they could enact their business plans.

The USG could take a variety of actions, as discussed below. These actions are not mutually exclusive.

Action 1: Specify Contract Terms for USG Purchases under Special Circumstances

A U.S. agency could contractually obtain exclusive rights to particular datasets from an RF collection company. This could be based on geographic collection areas, specific frequency ranges, or other criteria. This action would be analogous to "shutter control" in the satellite remote sensing industry.

Pros: The U.S. agency would be able to mandate procedures for data protection and specify auditing mechanisms to ensure the company is adhering to the contractual obligations and any related U.S. laws and regulations. This approach may not require any revisions to U.S. law, regulation, or policy.

Cons: Other commercial providers on the international market would not be subject to the same conditions. Similar to commercial satellite imagery, this approach would be costly and only be effective for as long as there are few service providers, most of which are subject to U.S. regulation. As the market grows, this tactic will yield diminishing returns. Additionally, it could be difficult to convince a provider to sell exclusive rights that are open-ended, in contrast to the imagery example, which was bound by both time and geography.

Action 2: Update or Replace U.S. Commercial Remote Sensing Policy to Include RF Collection

So much has changed since the national policy on satellite remote sensing (NSPD-27)[52] was issued in 2003 that this action essentially would mean starting from scratch on a new commercial remote sensing policy.

Pros: The RF collection issue provides another reason to initiate this update sooner rather than later. Some of the RF issues have analogies in commercial remote sensing, such as possible restrictions on the sale of certain types of product or information on sensitive domestic or allied sites. An update could address whether the sale of raw RF data, or data on certain frequency bands, should be restricted to the USG only or if there are particular global customers, in addition to already proscribed entities, that should be denied access to commercial RF products. Such questions and concerns would be thoroughly vetted in a new policy's interagency formulation process. The update could be accomplished by a new space policy directive on RF collection while leaving the remainder of NSPD-27 intact.

Cons: A rewrite of commercial remote sensing policy would be time consuming and labor intensive. It could get bogged down with issues unrelated to commercial RF collection and drag on for well over a year. If resolving RF collection issues is urgent, this could be better served by developing an implementation memorandum using the existing NSPD-27 language that would clarify the policy to include regulation of RF collection. Alternatively, a standalone policy may better address RF's unique features.

Action 3: Amend 51 U.S.C. Chapter 601 to Include RF Collection as Part of Commercial Remote Sensing

This action is based on an assumption that the two commercial activities are closely related and should be overseen by the same regulatory agency.

Pros: As noted above, there are some similarities between RF collection and imagery collection, particularly in national security and privacy concerns. The two could be addressed as one rather than creating separate statutory language. Commercial remote sensing space systems licensing and regulation already have useful structures in place, such as the interagency review process governed by the "Memorandum of Understanding Among the Departments of Commerce, State, Defense, and Interior, and the Office of the Director of National Intelligence, Concerning the Licensing and Operations of Private Remote Sensing Satellite Systems" (MOU), which makes DoC a suitable home for licensing commercial RF collections. Under this approach, a revised collaboration path, consistent with the amended rule, would be necessary.

Cons: Though similar, the technologies and concerns are not identical. The existing Commercial Remote Sensing Regulatory Affairs Office (CRSRA) in the Department of Commerce, for example, may or may not be the right choice for oversight of RF collection. Any RF sensing authorization program should leverage the expertise of all stakeholder agencies, including the DOD and the Office of the Director of National Intelligence or its subordinate agencies, especially the National Security Agency. Ideally, a broader, light-touch authorization program for new, emerging technologies, such as RF collection, would spur space innovation in the U.S. and clarify interagency roles in authorizing such operations.

This is a helpful model for the governance of commercial RF collections in that it identifies the relevant stakeholders, the process of review and escalation in case of disagreements, and timelines. However, RF collection has a different phenomenology that may require different agency and stakeholder participation and different technical experts. This could be accomplished with a new or amended MOU.

Action 4: Develop a New Space Policy Directive Covering Nontraditional Commercial Space Efforts

This action would assign licensing and regulatory responsibilities to an agency and begin developing procedures specific to commercial RF collection.

Pros: This action could be initiated quickly. It could allow for a variety of emergent technologies to be addressed that do not necessarily fit within the current remote sensing policy. Additionally, it could accelerate the effort to make the Office of Space Commerce into a one-stop shop for commercial space regulation.

Cons: Stakeholders in defense and intelligence agencies may lack confidence that this will allow them sufficient visibility into and influence over the regulatory decisionmaking process. Relevant committees in Congress may have similar concerns. However, the existing MOU could be used to establish appropriate coordination and consultation processes.

Once a lead agency is chosen, that agency and other USG stakeholders could collaborate to determine whether new regulations are needed and how they should be implemented. Recognition of existing laws (specifically, the Wiretapping Act and the Espionage Act, codified by 18 U.S. Code 2511) may lead to the conclusion that enforcement of current statutes is sufficient. Rather than establishing a new set of regulations, the licensing process for commercial RF collection could be limited to the lead agency educating the licensee on its responsibilities (with assistance from other stakeholder agencies, as appropriate) and verifying

that the licensee has strong mechanisms in place to ensure compliance with relevant laws.

This may be sufficient to address concerns of the national security community without enacting new regulations and attempting to apply them retroactively to early-to-market operators. The Wiretapping Act and Espionage Act in Title 18 already cover key privacy and national security concerns. For example:

- It is unlawful to intentionally intercept, use, or disclose electronic communications that are not readily accessible to or intended for use by the general public. There are exceptions in circumstances such as addressing signal interference and computer trespassing.
- Obtaining national defense information with intent or reason to believe that the information is to be used to injure the United States or, to the advantage of any foreign nation, shall incur fines or imprisonment of not more than ten years, or both.
- Attempting "to communicate, deliver, or transmit" intercepted information relating to the national defense to a foreign entity is punishable "by death or by imprisonment for any term of years or for life."

Action 5: Develop Norms and Guidelines in Collaboration with Industry

A guiding document could summarize legal and regulatory requirements. New and evolving norms could be promulgated through an industry standards body.

Pros: This could allow the greatest number of stakeholders to be involved in formulating governing protocols and take into account international partnerships, companies, and governing bodies. With industry involvement, protocols can better reflect the technical specifications and capabilities of existing and proposed RF collection systems. Importantly, there would be no added regulatory burden for companies. The U.S. guidance could be used to promulgate such norms of behavior to international actors.

Cons: New norms developed under this standards body would not be legally binding and would depend on education and compliance incentives from international governance bodies such as the International Telecommunication Union (ITU) along with U.S. agencies and professional associations. This would also

Creating and Promoting Standards

The **American National Standards Institute (ANSI)**,[53] a private, nonprofit organization that facilitates the development of consensus-based standards for a wide range of U.S. industries, could provide a venue for developing technical and procedural norms for the RF collection industry. ANSI's membership includes companies, government agencies, academic institutions, international bodies, other organizations, and individual professionals. This diversity allows stakeholders across a community of interest to participate in the process.

ANSI also promotes the use of U.S. standards internationally and advocates U.S. policy and technical positions in international and regional standards organizations. This could provide an avenue to address international advocacy for U.S. norms and guidelines for RF collection, an important objective identified by experts interviewed for this study.

One of the members of ANSI is the DoC's **National Institute of Standards and Technology (NIST)**, which conducts programs directly related to the technologies and markets of the commercial RF collection industry. NIST's Public Safety Communications Research Program (PSCR) works directly with first responders and researchers to address public safety needs in communications and state-of-the-art technologies, which could benefit from emergency response support offered by RF collection companies. Another NIST program, the National Advanced Spectrum and Communications Test Network (NASCTN), addresses spectrum-sharing challenges in the deployment of wireless technologies among commercial and federal users. This effort could take advantage of the spectrum mapping services offered by the industry.

require good faith involvement by private actors, including the application of peer pressure to bring noncompliant actors into line.

Conclusion

This report discusses the pros and cons of a variety of oversight actions the USG could take. These actions are not mutually exclusive, and not all of them may be required. Recent discussions with senior stakeholders appear to favor an approach using existing law and regulations already in place but no consensus had been achieved yet.

For decades, the USG operated on the assumption that RF collection from space was a USG-only activity. That assumption is no longer valid. Given that commercial RF collections from space are underway today, the time for deliberate actions to accomplish U.S. goals regarding such commercial activities has certainly arrived.

Acknowledgments

The authors would like to express their appreciation to Samira H. Patel of CSPS, who contributed to the research for this paper.

Appendix A
Privacy, Electronic Surveillance, and the Law

"**Invasion of privacy** is the intrusion into the personal life of another, without just cause, which can give the person whose privacy has been invaded a right to bring a lawsuit for damages against the person or entity that intruded. It encompasses workplace monitoring, Internet privacy, data collection, and other means of disseminating private information."[54]

The Supreme Court has ruled that there is a limited constitutional right to privacy. This includes privacy from surveillance in areas where a person has a "reasonable expectation of privacy," which can change with the advancement and proliferation of technology, as well as other factors. Privacy rights also are the subject of state laws, which vary from state to state. Privacy protections govern the actions of the U.S. government, state and local governments, and U.S. individuals and organizations.

U.S. law recognizes four categories of invasion of privacy of private individuals:

1. **Intrusion** on solitude or into private affairs (physical or electronic)

2. **Public disclosure of private information** which a reasonable person would find objectionable or embarrassing

3. Publication of facts that place a person in a **false light**

4. **Appropriation** and unauthorized use of a person's name or likeness

It is not immediately obvious how commercial satellite interception of RF signals could invade any of the four categories of privacy if the operators are faithful to their business plans and do not decode message content. Their AIS and search and rescue services detect signals from parties who want to be found. Spectral mapping and interference detection yield no information about individuals and mirror services that already are performed terrestrially. The potential privacy concern could be geolocation, used to pinpoint sources of interference and to track transportation, particularly in the maritime domain.

For privacy concerns, a possible analogy to satellite RF collection is the municipal use of cameras to monitor streets and other public areas. In both cases, the technology to monitor large areas continuously is relatively recent. The subjects being monitored typically are not aware of it, but even if they are, they have no means to approve or disapprove of each instance of monitoring that they experience. The significant difference is that municipal monitoring is a public service while commercial RF collection is done for profit (although companies' emergency services perform a public service).

Municipal video surveillance is considered to be legal as long as proper guidelines are followed. For example, the surveillance should not profile people based upon discriminatory profiling. Also, the surveillance should watch for problems that need attention, not chronicle the behavior patterns of specific people.[55] As experience is gained in satellite RF collection, government regulators and the stakeholder community can develop a similar set of guidelines with particular attention to geolocation and transportation monitoring functions. (Regarding interference detection and geolocation, Title 18 of the U.S. Code states that it is permissible to intercept any wire or electronic communication that is causing harmful interference to the extent necessary to identify its source.)

Relevant Supreme Court rulings over the past half-century highlight some points to consider regarding U.S. government use of commercial satellite RF collection services and the government's responsibility to regulate such services:

- Satellite RF collection systems likely would be deemed "sophisticated" and "not in general public use" in a domestic court case challenging their use. They could be depicted as invasive tools of the government. However, this view may be short-lived if RF collection services become more common and can be purchased by anyone willing to pay. This is analogous to the evolution of high-resolution satellite imagery during the past 20 years.

- U.S. courts could see potential for significant erosion of Fourth Amendment rights (regarding search and seizure) from both passive and active sensor systems. Advancements in technical capabilities could improve location tracking or increase the amount of detail that can be detected about individuals or inside enclosures without physical intrusion.

- Subjects being observed would have no means of detecting the surveillance, making them unwitting victims of intrusion in the eyes of the court.

- There would be no legal recourse to ban overflights of spacecraft, as might be the case for private aircraft or drones.

- The important factors in U.S. government use of commercial RF collection services are what is being collected, how it is used, and how it is stored and shared, not who owns the collection system.

Appendix B
Non-U.S. Signals Intelligence Laws and Regulations

Legislation and regulations relevant to signals collection proliferated in the past decade. This has been driven by multiple factors, the most prominent of which seems to be responses to terrorist incidents and threats and the general movement toward better-defined and more stringent privacy laws. Additionally, the Edward Snowden information leaks prompted self-examination in many countries. For example, the European Parliament in 2014 passed a resolution calling on "the US authorities and the EU Member States…to prohibit blanket mass surveillance activities" and calling on "the EU Member States to comprehensively evaluate, and revise where necessary, their national legislation and practices governing the activities of the intelligence services" and "ensure that their current or future legislative frameworks and oversight mechanisms governing the activities of intelligence agencies are in line with the standards of the European Convention on Human Rights and European Union data protection legislation."[56] This came on the heels of a U.N. General Assembly resolution urging U.N. members to review their legislation on secret surveillance.[57]

As the brief examples below indicate, this activity has been aimed at government SIGINT collection. Although the European Union's General Data Protection Regulation (discussed below) addresses data collection by nongovernment entities, no evidence exists that legislators or regulatory authorities have directed their attention specifically to commercial SIGINT collection and, particularly, space-based collection. Foreign governments instead have focused their attention on data collected by businesses and other organizations and on social media, which can be misused by the collectors or by data thieves.

In **France**, communications interception is carried out primarily by the Directorate General on Exterior Security under the Ministry of Defense. The metadata collected is shared among the six agencies that make up the French intelligence network, all of which were created by executive action. The July 2015 adoption of the Law on Intelligence constitutes the most comprehensive legislative effort to date that regulates the activities of the intelligence agencies.

Communications interception is governed by the Code of Domestic Security, as amended by recent laws such as the Law on Intelligence and the Law on International Electronic Communications Measures. The code addresses privacy guarantees but also provides for interception in circumstances where national security and other safety-related concerns are at issue. The National Commission for the Control of Intelligence Techniques has oversight of interception surveillance, but its recommendations do not appear to be binding.[58]

In **Germany**, Article 10 of the Basic Law (Constitution) provides that the privacy of correspondence, mail, and telecommunications is "inviolable." Restrictions on privacy may only be imposed pursuant to laws protecting societal freedom and security.

There are three intelligence agencies at the federal level, two of which focus on domestic intelligence and a third, the Federal Intelligence Service, which focuses on foreign intelligence. Intelligence gathering in Germany is regulated by the acts that established the three federal intelligence agencies and the Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications. The intelligence agencies are subject to extensive administrative as well as general and specialized parliamentary oversight.

Following the September 11, 2001, terrorist attacks and the subsequent terrorist attacks in Madrid and London, federal law enforcement agencies were given preventive powers (including the authority to intercept communications) to protect against homegrown terrorists. Agencies granted such powers include the Federal Criminal Police Office, the Federal Police, and the Customs Investigation Bureau and Customs Investigation Offices. In June 2016, in reaction to terrorist attacks in Paris and Istanbul, the federal government moved to amend several laws in order to improve information sharing between national and foreign agencies fighting terrorism.[59]

Legislative reforms in December 2016 imposed additional requirements for most foreign intelligence collection, including authorization by a panel of judges for such collection. Also, collection targets are now classified into four different groups requiring different authorization procedures, data protection standards, and oversight provisions. The groups (from most to least restrictive) are:

1. German citizens at home and abroad, all persons on German territory, and domestic legal entities
2. Public institutions of EU bodies and member states
3. EU citizens
4. Rest of the world[60]

Telecommunications providers are required to comply with legal requests for subscriber data. Other aspects of private-sector behavior related to signals collection do not appear to be addressed in statutes.

In **Sweden**, the Foreign Intelligence Inspectorate, led by a government-appointed board, oversees all of the country's foreign intelligence activities. The National Defense Radio Establishment (FRA) is the only agency authorized to carry out signal surveillance, and only on cross-border communications, governed by the Act on Signal Surveillance for Defense Intelligence Activities.[61]

Although the rules prohibit surveillance targeting of a single individual, mass surveillance is permitted and has been enabled by a statutory change that took effect in 2009. This has drawn criticism from the European Parliament and other commenters that believe Sweden's practices violate the European Convention for the Protection of Human Rights and Fundamental Freedoms. Despite this, in 2018 the European Court of Human Rights upheld Sweden's legislation authorizing covert bulk signals collection.[62]

A **European Union** directive on data privacy, adopted in 1995, addressed electronic interception and surveillance.[63] These actions are permitted on the grounds of national security and the prevention, investigation, detection, and prosecution of criminal offenses or unauthorized use of an electronic communications system.[64] The 1995 directive was superseded by the General Data Protection Regulation (GDPR), which came into force in May 2018. The most significant changes in the GDPR are increased penalties for violations and greater territorial scope. (Companies outside the EU are covered by the regulation as well.)[65]

The GDPR, which protects individuals sharing data through commercial transactions or on social media channels, is applicable to companies that collect, store, or process personal data, which is not applicable to current RF collection business plans. The regulation defines "personal data" as "any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier." The only data collected by HawkEye 360, for example, that could fit this definition is emergency locator signals that would be picked up in search-and-rescue operations. But this is an obvious exception since the individual is broadcasting the information with the desire to be

located. The definition does not include spectrum mapping, geolocation of interference, or maritime domain awareness, so the regulation should not affect commercial RF collectors unless their technology and business plans change to include personal data.

The difficulty in interpreting EU regulations is illustrated by a recent court ruling on a case brought against the government of the United Kingdom. In September 2018, the European Court of Human Rights found that the U.K. violated some parts of the European Convention on Human Rights by conducting bulk interception of communications signals and obtaining communications data from service providers. The violations were deemed to be a result of inadequate oversight and safeguards for the collected data. However, the court found that bulk interception itself did not violate the convention. Although this case addresses the actions of a government agency, it could raise questions for commercial RF collectors regarding what constitutes adequate oversight and safeguards.[66]

Japan's constitution provides for a general right to privacy, and wiretapping of landlines is prohibited by law unless there is a court order. However, interception of wireless communications, including those involving satellites, is a gray area with no legal precedent for limitation.[67]

References

[1] HawkEye 360, "HawkEye 360 Products and Applications" (https://www.he360.com/products/).

[2] HawkEye 360, "HawkEye 360 Applications" (https://www.he360.com/resources/).

[3] Navigation Center, United States Coast Guard, "AIS References" (www.navcen.uscg.gov/pdf/AIS/AIS_Regs_SOLAS_MTSA_FR.pdf).

[4] exactEarth, "AIS Vessel Tracking | Maritime Ship Monitoring" (www.exactEarth.com/).

[5] Herbert J. Kramer, "HawkEye 360 Pathfinder Cluster Mission to Identify RFI Locations," HawkEye - Satellite Missions, EoPortal, (https://directory.eoportal.org/web/eoportal/satellite-missions/h/HawkEye).

[6] HawkEye 360, "Satellites, Geolocation-RF Signal Detection-Applications, Search/Rescue, AIS" (www.he360.com/products/).

[7] Kratos Defense and Security Solutions Inc., "Kratos and HawkEye 360 Announce Collaboration to Advance Spectrum Detection, Characterization, and Geolocation Services" (http://ir.kratosdefense.com/news-releases/news-release-details/kratos-and-hawkeye-360-announce-collaboration-advance-spectrum).

[8] CRFS Spectrum Monitoring and Geolocation (https://www.crfs.com/).

[9] HawkEye 360, "HawkEye 360 Announces Successful Launch of First Three Satellites," December 4, 2018 (www.he360.com/hawkeye-360-announces-successful-launch-of-first-three-satellites/).

[10] Allied Minds, "HAWKEYE 360 Commercialising Space-Based Precision RF Detection and Analytics," January 2018 (www.investors.alliedminds.com/~/media/Files/A/Allied-Minds-IR/reports-and-presentations/hawkeye-360-cmd-presentation.pdf).

[11] Debra Werner, "Ursa Space Systems and HawkEye 360 fuse radar, RF," *SpaceNews*, June 4, 2019 (https://spacenews.com/ursa-hawkeye-partnership/).

[12] Debra Werner, "Hawkeye 360 and Windward to offer new maritime product," *SpaceNews*, May 22, 2019 (https://spacenews.com/hawkeye-360-windward/).

[13] HawkEye 360, "Radio Frequency (RF) Signal Detection, Spectrum Mapping and Management" (www.he360.com/products/RFGeo/).

[14] Gunter's Space Page - Information on Spaceflight, Launch Vehicles and Satellites, "THEA" (www.space.skyrocket.de/doc_sdat/thea.htm).

[15] Aurora Insight, "Spectrum and Wireless Infrastructure Intelligence" (www.aurorainsight.com/).

[16] SpaceQuest Ltd, "S-AIS Data" (www.spacequest.com/s-ais).

[17] Kleos Space Commercial Applications (http://kleos.space/commercial/).

[18] ASX and Media Release, KLEOS, "Kleos Space Signs Contract with Rocket Lab to Launch the Kleos Scouting Mission Satellites" (www.asx.com.au/asxpdf/20180920/pdf/43ygz7grrz97my.pdf); Debra Werner, "Kleos Space prepares to launch RF monitoring constellation," *Space News*, June 4, 2019 (https://spacenews.com/kleos-prepares-launch/); Doug Messier, "Kleos Scouting Mission Launch Period Extended", *Parabolic Arc*, July 22, 2019 (http://www.parabolicarc.com/2019/07/22/kleos-scouting-mission-launch-period-extended/).

[19] Kleos Space, "Products" (www.kleos.space/commercial/).

[20] UNSEENLABS, "UNSEENLABS – The Bright Sight" (www.unseenlabs.space/).

[21] GOMspace, "GomSpace Selected by UnseenLabs for the Turn-Key Delivery of a Disruptive Spectrum Monitoring System" (www.gomspace.com/news/gomspace-selected-by-unseenlabs-for-the-turn-.aspx).

[22] Doug Mohney, "Radio Sensor Nanosatellites Opening New Opportunities," *Space IT Bridge*, June 1, 2018 (www.spaceitbridge.com/radio-sensor-nanosatellites-opening-new-opportunities.htm).

[23] Adelis-SAMSON Projects | Distributed Space Systems Lab (www.dssl.technion.ac.il/Adelis-SAMSON).

[24] Gunter's Space Page - Information on Spaceflight, Launch Vehicles and Satellites, "SAMSON 1, 2, 3" (www.space.skyrocket.de/doc_sdat/samson.htm).

[25] https://www.crfs.com/.

[26] https://www.horizontechnologies.eu/.

[27] U.S. Air Force, "RQ-4 Global Hawk," Fact Sheet, October 27, 2014 (https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/).

[28] James A. Vedda and Peter L. Hays, "Major Policy Issues in Evolving Global Space Operations," The Aerospace Corporation, Center for Space Policy and Strategy, December 2017, pp. 42-48 (https://aerospace.org/sites/default/files/2018-05/Space_Policy_FINAL_interactive_0.pdf).

[29] Josef Koller, "The Future of Ubiquitous, Realtime Intelligence: A GEOINT Singularity," CSPS Publication, 2019, (https://aerospace.org/paper/future-ubiquitous-realtime-intelligence-geoint-singularity).

[30] Katz v. United States, 389 U.S. 347 (1967) (https://supreme.justia.com/cases/federal/us/389/347/).

[31] Dow Chemical Co. v. United States, 476 U.S. 227 (1986) (https://supreme.justia.com/cases/federal/us/389/347/).

[32] Danny Lee Kyllo, Petitioner v. United States, 533 U.S. 27 (2001) (https://supreme.justia.com/cases/federal/us/533/27/).

[33] Andrew Crocker & Jennifer Lynch, "Victory! Supreme Court Says Fourth Amendment Applies to Cell Phone Tracking," Electronic Frontier Foundation, June 22, 2018 (https://www.eff.org/deeplinks/2018/06/victory-supreme-court-says-fourth-amendment-applies-cell-phone-tracking). The Supreme Court opinion on this case can be found at https://www.eff.org/document/carpenter-v-united-states-supreme-court-opinion.

[34] Public Law 102-555, "Land Remote Sensing Policy Act of 1992," October 28, 1992 (https://www.congress.gov/bill/102nd-congress/house-bill/6133).

[35] House Report No. 102-539, 102nd Congress, 2nd Session, May 28, 1992.

[36] Senate Report No. 102-445, 102nd Congress, 2nd Session, September 30, 1992.

[37] Department of Commerce Proposed Rule Making for Licensing of Private Remote Sensing Space Systems, NOAA-NESDIS-2018-0085.

[38] Code of Federal Regulations, 15 CFR 960.3, April 25, 2006 (https://www.ecfr.gov/cgi-bin/text-idx?SID=0a34184fd0e89e876b0ecd908a29652c&mc=true&node=se15.3.960_13&rgn=div8).

[39] National Oceanic and Atmospheric Administration, "Licensing of Private Remote Sensing Space Systems," Proposed Rule, 84 FR 21282, May 14, 2019 (https://www.federalregister.gov/documents/2019/05/14/2019-09320/licensing-of-private-remote-sensing-space-systems).

[40] U.N. Principles Relating to Remote Sensing of the Earth from Outer Space (http://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/remote-sensing-principles.html).

[41] National Space Policy of the United States of America, June 28, 2010 (https://www.nasa.gov/sites/default/files/national_space_policy_6-28-10.pdf).

[42] Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. §2510-2713 and §3101-3127 (http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter119&edition=prelim).

[43] Unauthorized publication or use of communications, 47 U.S.C. §605 (https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title47-section605&num=0&edition=prelim).

[44] 50 U.S.C. §1801-1811 (http://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter36/subchapter1&edition=prelim).

[45] Foreign Intelligence Surveillance's (FISA's) lengthy definition of electronic surveillance essentially describes it as communications intelligence by any mechanical or electronic means.

[46] Public Law 107-56, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (http://uscode.house.gov/statutes/pl/107/56.pdf).

[47] Executive Order 12333, "United States Intelligence Activities," December 4, 1981 (https://www.archives.gov/federal-register/codification/executive-order/12333.html).

[48] DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010 (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510020p.pdf).

[49] DoD Instruction O-3115.07, "Signals Intelligence (SIGINT)," September 15, 2008 (https://directives.whs.mil/issuances/O311507p.pdf).

[50] USSID SP0018, "United States Signals Intelligence Directive," Office of the Director of National Intelligence, January 26, 2011 (www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf).

[51] Bureau of Industry and Security, "Recently Published Regulations" (https://www.bis.doc.gov/index.php/regulations).

[52] National Security Presidential Directive 27, "U.S. Commercial Remote Sensing Policy," April 25, 2003.

[53] ANSI webpage (https://www.ansi.org/about_ansi/).

[54] USLegal.com, "Invasion of Privacy Law and Legal Definition"

(https://definitions.uslegal.com/i/invasion-of-privacy/).

[55] Cliff Rieders, "Public Surveillance and Your Legal Right to Privacy," *The Legal Intelligencer*, February 28, 2019 (https://www.law.com/thelegalintelligencer/2019/02/28/public-surveillance-and-your-legal-right-to-privacy/?slreturn=20190720133227).

[56] European Parliament, "Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs," 2013/2188(INI), March 12, 2014 (http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN&ring=A7-2014-0139).

[57] U.N. General Assembly, "The Right to Privacy in the Digital Age," G.A. Res. 68/167, U.N. Doc A/RES/68/167, December 18, 2013 (http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167).

[58] U.S. Law Library of Congress, "Foreign Intelligence Gathering Laws," June 2016, pp. 8-14 (https://www.loc.gov/law/help/intelligence-activities/intelligence-gathering.pdf).

[59] Ibid., pp. 15-24.

[60] Thorsten Wetzling, "New Rules for SIGINT Collection in Germany: A Look at the Recent Reform," *Lawfare*, June 23, 2017 (https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform).

[61] U.S. Law Library of Congress, "Foreign Intelligence Gathering Laws," pp. 42-46.

[62] Asaf Lubin, "Legitimizing Foreign Mass Surveillance in the European Court of Human Rights," *JustSecurity.org*, August 2, 2018 (https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/).

[63] U.S. Law Library of Congress, "Foreign Intelligence Gathering Laws," pp. 65-76.

[64] European Innovation Partnership on Active and Healthy Ageing, Directive 95/46/EC (https://ec.europa.eu/eip/ageing/standards/ict-and-communication/data/directive-9546ec_en).

[65] General Data Protection Regulation (GDPR) FAQs (https://eugdpr.org/the-regulation/gdpr-faqs/).

[66] European Court of Human Rights, "Some aspects of UK surveillance regimes violate Convention," press release, September 13, 2018 (https://hudoc.echr.coe.int/app/conversion/pdf?library=ECHR&id=003-6187848-8026299&filename=Big%20Brother%20Watch%20and%20Others%20v.%20the%20United%20Kingdom%20%20-%20complaints%20about%20surveillance%20regimes.pdf).

[67] Ryan Gallagher, "The Untold Story of Japan's Secret Space Agency," *The Intercept*, May 19, 2018 (https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/).