



**COMMENTS OF THE
ELECTRONIC FRONTIER FOUNDATION
REGARDING PROPOSED RULE FOR LICENSING OF
PRIVATE REMOTE SENSING SPACE SYSTEMS**

NOAA-NESDIS-2018-0058

Docket No: 100903432-9396-01

84 Fed. Reg. 21282

Submitted on July 15, 2019 to the Department of Commerce, the National Oceanic and Atmospheric Administration, and the National Environmental Satellite, Data, and Information Service

The Electronic Frontier Foundation (EFF) is grateful for the invitation from the Department of Commerce (Commerce) and the National Oceanic and Atmospheric Administration (NOAA) to comment on the proposed rule for licensing of private remote sensing space systems, and would like to use this opportunity to highlight the privacy implications of data collected by these systems and Commerce’s mandate that this data must be shared with governments around the world.

EFF is a non-profit organization that has worked for almost 30 years to protect civil liberties, privacy, consumer interests, and innovation in new technologies. EFF actively encourages and challenges the executive and judiciary to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. With more than 31,000 contributing members, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

I. Summary

The Department of Commerce (Commerce), through the National Oceanic and Atmospheric Administration (NOAA), licenses the operation of private “remote sensing space systems”—commonly referred to as satellites—under the Land Remote Sensing Policy Act of 1992.¹ NOAA’s existing regulations implementing the Act were last updated in 2006.² NOAA is now proposing to rewrite those regulations, and, as part of its rulemaking proceeding, has requested public comment on the new proposed regulations.

¹ 51 U.S.C. 60101 et seq.

² *Meeting Minutes: 25th Meeting of the Advisory Committee on Commercial Remote Sensing (ACCRES)*, at 3 (2019), https://www.nesdis.noaa.gov/CRSRA/pdf/ACCRES_25th_Meeting_Minutes_Final_070119.pdf.

In June 2019, Commerce Secretary Wilbur Ross stated that the “space economy” is projected to grow to \$3 trillion by 2040.³ To ensure the United States remains the leader in this field, Secretary Ross stated that “[r]egulations must be modified to ensure the competitiveness of the industry.”⁴ Through its proposed rule, NOAA intends to modify existing regulations to make it easier for private entities to obtain licenses and to reduce compliance burdens for licensees.⁵ To accomplish this goal, the rule creates two categories for licenses—low and high-risk—determined by impact on the “national security and international obligations of the United States.”⁶ All applications (whether low or high-risk) will be afforded a presumption of approval.⁷ NOAA anticipates that most applications will not have to go through further individualized interagency review, which will be reserved for applicants who present a novel risk that cannot be addressed by its standard licensing conditions.⁸

Private satellites have useful, societally beneficial functions. Satellite images have been leveraged for research, commercial, and government uses, including tracking global oil stockpiles, measuring deforestation in the Amazon, and identifying boats engaged in illegal fishing.⁹ They have also been used to illuminate human rights abuses, providing evidence of labor camps in North Korea and Boko Haram attacks in Nigeria.¹⁰

However, the same technology that exposes human rights abuses can also be used to perpetuate them. NOAA’s proposed rule continues its preexisting practice of requiring—as a condition of its grant of a license—government access to unenhanced data collected by private satellites. Both low and high-risk applicants must, upon request, provide unenhanced data to “the government of any country (including the United States)” if the data cover that country’s territory, “unless doing so would be prohibited by law or license conditions.”¹¹

Although the proposed rule addresses cybersecurity by requiring low and high-risk applicants to implement National Institute of Standards and Technology (NIST)-approved encryption methods, it does not address privacy and civil liberties concerns.¹² Satellites are capable of highly advanced and continuous surveillance through high

³ *Id.*

⁴ *Id.*

⁵ Licensing of Private Remote Sensing Space Systems, 84 Fed. Reg. 21282, 21283 (proposed May 14, 2019) (to be codified at 15 C.F.R. pt. 960).

⁶ *Id.*

⁷ 84 Fed. Reg. at 21286.

⁸ 84 Fed. Reg. at 21285.

⁹ Aaron Clark et al., *All the Things Satellites Can Now See From Space*, Bloomberg Businessweek (July 26, 2018), <https://www.bloomberg.com/news/features/2018-07-26/all-the-things-satellites-can-now-see-from-space>.

¹⁰ Naomi Larsson, *How satellites are being used to expose human rights abuses*, The Guardian (Apr. 4, 2016) <https://www.theguardian.com/global-development-professionals-network/2016/apr/04/how-satellites-are-being-used-to-expose-human-rights-abuses>.

¹¹ 84 Fed. Reg. at 21292, 21294.

¹² 84 Fed. Reg. at 21293-94.

resolution imaging, thermal imaging, and near real-time video, and their capabilities are increasing every day. They can amass large amounts of archived data on private citizens, which allows anyone with access to the data the ability to enter a virtual time machine and view and track actions that occurred in the past.

By combining this data with other information, one could deduce a detailed log of a person's movements for as long as a satellite operator retains data. As the Supreme Court recently recognized in a case addressing the collection of historical location information, "time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"¹³ According to NOAA's rule, data gathered by private satellites must be shared with governments upon request. However, unchecked government access to such data implicates the exact privacy and civil liberties concerns the Supreme Court highlighted in *Carpenter*. For this reason, EFF asks NOAA to incorporate privacy protections into private satellite licensing.

II. Privacy Considerations for Data Collected by Private Satellites

Satellite technology, and specifically its capacity for surveillance, is quickly advancing. Satellites already have the ability to take high resolution images, create thermal images, and record video, and satellite systems are only becoming cheaper, more sophisticated, and more prevalent.¹⁴ Companies also hold archives of data received by private satellites. Although private satellite technology has not yet advanced to the point of being able to identify individuals, existing and imminent capabilities raise significant privacy and civil liberties risks.

Satellites have powerful imaging capacity, and private satellites are currently allowed to create private images of up to 25 centimeters of resolution.¹⁵ Satellite images at that resolution allow viewers to discern individual mailboxes.¹⁶ United States government surveillance satellites, which are not subject to the same resolution regulations as private satellites, are able to discern objects that are less than 10 centimeters wide.¹⁷ At this resolution, a satellite can make out the contours of someone's head.¹⁸

¹³ *Carpenter v. U.S.*, 138 S. Ct. 2206, 2217 (2018) (quoting *U.S. v. Jones*, 565 U.S. 400, 415 (2012)).

¹⁴ In 2017, the cost of launching a satellite was comparable to the cost of developing and launching a smartphone app. Bernard Marr, *Why Space Data Is The New Big Data*, *Forbes* (Oct. 19, 2017), <https://www.forbes.com/sites/bernardmarr/2017/10/19/why-space-data-is-the-new-big-data/#791e229069a1>.

¹⁵ Kelly Dickerson, *Companies want to launch satellites that can see a phone in your hand from space*, *Business Insider* (Oct. 12, 2015), <https://www.businessinsider.com/satellite-image-resolution-keeps-improving-2015-10>; Ziya Tong, *Satellites Are Quietly, Constantly Watching Us*, *Vice Motherboard* (Jun. 11, 2019), https://www.vice.com/en_us/article/ywyxxm/how-satellites-quietly-constantly-surveil-us.

¹⁶ Dickerson, *supra*.

¹⁷ *Id.*

¹⁸ *Id.*

Satellites' surveillance capacities also depend on how high these satellites are launched. Most Earth observation satellites operate at low Earth orbit (LEO).¹⁹ A single one of these satellites can orbit around the Earth revisiting the same area every 90 minutes.²⁰ Geostationary orbit (GEO) satellites are launched much higher and can cover up to a third of Earth's land mass, but remain in the same fixed area.²¹ Although there are trade-offs between these satellites, some organizations are launching LEO satellites in grouped constellations, greatly expanding their coverage areas.²²

Satellites can also conduct thermal imaging, hyperspectral imaging, and atmospheric monitoring.²³ Hyperspectral images can "capture electromagnetic wavelengths outside the visible spectrum," and could be used by governments to "identify underground bunkers or nuclear materials."²⁴ Synthetic aperture radar technology gives satellites the enhanced ability to cut through cloud cover and determine the height of objects.²⁵

This imaging technology is rapidly progressing, becoming cheaper and easier to use. The number of Earth observation satellites has increased more than five times since 2008.²⁶ New nanosatellites, which are the size of toasters, are much cheaper to launch into space than conventional satellites.²⁷ The costs have decreased enough that at least one company is planning to schedule regular monthly launches that will transport multiple satellites into orbit at one time.²⁸ Moreover, demand for higher-resolution images is putting pressure on U.S. regulators to relax their 25 centimeter restriction.²⁹

Satellites currently can record video and will soon be able to take real-time video. EarthNow, a startup funded by Bill Gates, plans on becoming "the first satellite imaging system designed expressly to deliver real-time, intelligent video observations of the

¹⁹ Tong, *supra*.

²⁰ *Id.*

²¹ Stewart Sanders, *The new space race is all about satellites: Pros and cons of each orbit*, The Next Web (Nov. 3, 2018), <https://thenextweb.com/contributors/2018/11/03/the-new-space-race-is-all-about-satellites-pros-and-cons-of-each-orbit/>.

²² Sandra Erin, *Top general says large constellations of satellites in low orbit could address key needs*, Space News (Jun. 18, 2019), <https://spacenews.com/top-general-says-large-constellations-of-satellites-in-low-orbit-could-address-key-needs/>; Kakaes et al., *The number of satellites orbiting Earth could quintuple in the next decade*, MIT Technology Review (Jun. 29, 2019), <https://www.technologyreview.com/s/613746/satellite-constellations-orbiting-earth-quintuple/>.

²³ Jeffrey Lin & P.W. Singer, *Gaofen 4, The World's Most Powerful GEO Spy Satellite, Continues China's Great Leap Forward Into Space*, Popular Science (Jan. 8, 2016), <https://www.popsci.com/gaofen-4-worlds-most-powerful-geo-spy-satellite-continues-chinas-great-leap-forward-into-space/>.

²⁴ Christopher Beam, *Soon, satellites will be able to watch you everywhere all the time*, MIT Technology Review (Jun. 26, 2019), <https://www.technologyreview.com/s/613748/satellites-threaten-privacy/>.

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

²⁸ Jonathan O'Callaghan, *Rocket Lab to Launch Multiple Satellites On A Rideshare Mission Next Month*, Forbes (May 11, 2019), <https://www.forbes.com/sites/jonathanocallaghan/2019/05/11/rocket-lab-to-launch-multiple-satellites-on-a-rideshare-mission-next-month/#7040fb762344>.

²⁹ *Id.*

Earth.”³⁰ According to EarthNow, existing satellite technology is only able to deliver delayed video clips, but EarthNow plans to provide the first technology that will be able to deliver video in real-time.³¹ Enough satellites “will be deployed to ensure that at least one EarthNow satellite is always above areas of coverage,” making continuous coverage possible.³²

Several commercial satellite companies offer consumers the ability to search their archives for past imagery. DigitalGlobe, a satellite company that has collected images since 2001, allows customer access to every image they have taken.³³ As of 2017, it has amassed 100 petabytes of storage, increasing by 10 petabytes per year—enough data that it now contracts out data storage to Amazon Web Services.³⁴ Similarly, Planet Labs allows customers access to archive images dating back to 2009.³⁵

Data from these private satellites fit into a broader pattern of aerial surveillance already being used by law enforcement. For example, Persistent Surveillance Systems runs high-resolution cameras attached to planes that record city residents from above.³⁶ Its goal is to provide police with the ability to sift through footage, allowing them to rewind and zoom in to identify individuals’ locations.³⁷ In 2016, Persistent tested its technology in Baltimore, providing information to the police, the FBI, and the Secret Service without notifying residents.³⁸ In 2012, Persistent outraged Compton officials and residents by testing the same technology without providing public notice; in fact, a sergeant at the L.A. County Sheriff’s office explicitly said that the program was kept secret to avoid privacy-related scrutiny.³⁹

Combined with other law enforcement surveillance tactics, information generated from satellites could identify individuals. These tactics include aerial surveillance like Persistent’s technology, data generated from automated license plate readers,⁴⁰ cell phone data,⁴¹ street-level surveillance cameras,⁴² and facial recognition technology.⁴³ The

³⁰ *Frequently Asked Questions*, EarthNow (2018), <https://earthnow.com/>.

³¹ *Id.*

³² *Id.*

³³ Jay Littlepage, *DigitalGlobe moves to the cloud with AWS Snowmobile*, DigitalGlobe (May 17, 2010), <http://blog.digitalglobe.com/industry/digitalglobe-moves-to-the-cloud-with-aws-snowmobile/>.

³⁴ *Id.*

³⁵ *Planet Imagery and Archive*, Planet Labs (2019), <https://www.planet.com/products/planet-imagery/>.

³⁶ Conor Friedersdorf, *Mass Surveillance is Coming to a City Near You*, The Atlantic (Jun. 21, 2019), <https://www.theatlantic.com/ideas/archive/2019/06/mass-surveillance-tech/592117/>.

³⁷ *Id.*

³⁸ *Id.*

³⁹ Angel Jennings et al., *Sheriff’s secret air surveillance of Compton sparks outrage*, LA Times (Apr. 23, 2014), <https://www.latimes.com/local/lanow/la-me-ln-sheriffs-surveillance-compton-outrage-20140423-story.html>; Conor Friedersdorf, *Eyes Over Compton: How Police Spied on a Whole City*, The Atlantic (Apr. 21, 2014), <https://www.theatlantic.com/national/archive/2014/04/sheriffs-deputy-compares-drone-surveillance-of-compton-to-big-brother/360954/>.

⁴⁰ *Automated License Plate Readers*, EFF, <https://www.eff.org/pages/automated-license-plate-readers-alpr>.

⁴¹ *Cell-Site Simulators/IMSI Catchers*, EFF, <https://www.eff.org/pages/cell-site-simulatorsimsi-catchers>.

⁴² *Surveillance Cameras*, EFF, <https://www.eff.org/pages/surveillance-cameras>.

⁴³ *Face Recognition*, EFF, <https://www.eff.org/pages/face-recognition>.

Supreme Court recognized the particular danger of combining data in *Carpenter* when it pointed out that even if cell-site location information was not refined enough to precisely identify an individual's exact location, the government could create a "detailed log of Carpenter's movements" when CSLI was "combin[ed] with other information."⁴⁴

All of these functions of satellites raise clear privacy risks. Governments can use images and video from satellites to monitor our activities, and searchable archives can help them track this activity over time and dating back years into the past. With the advent of real-time video, private satellites could subject the entire world to continuous 24/7 surveillance. The Supreme Court has expressed Fourth Amendment concerns about surveillance that reaches inside the home (including via thermal imaging),⁴⁵ surveillance that logs travel in public,⁴⁶ surveillance over time that allows law enforcement to look back in time,⁴⁷ and the ability to surveil everyone⁴⁸—all surveillance concerns that are implicated by private satellites.

III. Incorporating Privacy Protections into Private Satellite Licensing

Private satellites raise clear privacy and civil liberties risks that NOAA should address in their proposed rule. Changes to this rule should include, at a minimum:

Expand disclosure of privacy risks in satellite licensing applications—Currently, NOAA requires applicants to submit information on resolution capacity, ability to capture video, and who owns, controls, or manages the system other than the licensee.⁴⁹ The new rule should require licensees to include more detailed information that speaks to the system's privacy risks, such as who the licensee is planning on sharing data with and for what purposes.

Conduct regular audits on which governments have asked for what data—Because the existing and proposed rules require satellite operators to provide data upon request to any government whose territory is observed, the new rule should require satellite operators to log and record data requests from governments in a way that assures transparency and to report these to the public on at least an annual basis. Operators should be required to conduct privacy assessments both before launching systems and every time use of system data changes to ensure that governments are using this data responsibly and ethically.

Incorporate privacy considerations in the criteria for determining low and high-risk applicants—In the proposed rule, resolution capacity and ability to capture video

⁴⁴ *Carpenter*, 138 S. Ct. at 2218.

⁴⁵ *Kyllo v. U.S.*, 533 U.S. 27, 40 (2001)

⁴⁶ *Carpenter*, 138 S. Ct. at 2217-18; *U.S. v. Jones*, 565 U.S. 400, 404, 414-15 (2012).

⁴⁷ *Carpenter*, 138 S. Ct. at 2218.

⁴⁸ *Carpenter*, 138 S. Ct. at 2218-19.

⁴⁹ 84 Fed. Reg. at 21297.

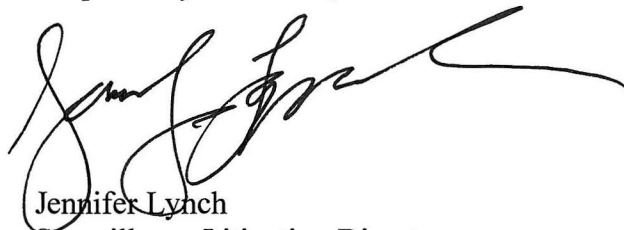
inform whether an application is “high-risk,” but other privacy risks do not.⁵⁰ Additional privacy risks should be factors in whether NOAA determines a system is “high risk.” For example, if companies are targeting law enforcement agencies or foreign governments with known human rights violations as customers for their images, that should be a factor that triggers high-risk classification.

Consider further rulemaking on the privacy concerns around private satellites—Assessment of privacy risks would benefit from discussion with more stakeholders, including non-governmental organizations and representatives from communities most likely to be impacted by invasive satellite surveillance. NOAA should consider conducting a separate rulemaking that addresses the privacy and civil liberties risks of private satellites, which would invite ideas and comments from a broader group of interested parties.

IV. Conclusion

NOAA has recognized that increasing transparency is a “shared goal” of the current Administration and the public.⁵¹ To adequately meet this goal, EFF respectfully urges NOAA to adopt the recommendations listed above. Private satellites raise clear privacy and civil liberties risks, and the American public and legislators will benefit from greater transparency around the uses of private satellites, including whether and how the data they collect is shared with government agencies around the world.

Respectfully submitted,



Jennifer Lynch
Surveillance Litigation Director
Electronic Frontier Foundation

⁵⁰ 84 Fed. Reg. at 21291.

⁵¹ 84 Fed. Reg. at 21282.