
The Role of Satellites and Smart Devices: Data Surprises and Security, Privacy, and Regulatory Challenges

Anne Toomey McKenna,^{*i} Amy C. Gaudion,^{**ii}
Jenni L. Evans^{***iii}

ABSTRACT

Strava, a popular social media platform and mobile app like Facebook but specifically designed for athletes, posts a “heatmap” with consensually-obtained details about users’ workouts and geolocation. Strava’s heatmap depicts aggregated data of user location and movement by synthesizing GPS satellite data points and movement data from users’ smart devices together with satellite imagery. In January of 2018, a 20-year-old student tweeted that Strava’s heatmap revealed U.S. forward operating bases. The tweet revealed a significant national security issue and flagged substantial privacy and civil liberty concerns.

Smart devices, software applications, and social media platforms aggregate consumer data from multiple data collection sources, including device-embedded sensors, cameras, software, and GPS chips, as well as from consumer activities like social media posts, pictures, texts, email, and contacts. These devices and apps utilize satellite data, including GPS, as a fundamental component of their data collection arsenal. We call this little understood, across-device, across-platform, and multi-sourced data aggregation the *satellite-smart device information nexus*. Given the nature of the technology and data aggregation, no one escapes the satellite and smart device information nexus. We explain the technology behind both

^{*}**Anne Toomey McKenna** is Penn State Dickinson Law’s Distinguished Scholar of Cyber Law and Policy and co-hire with Penn State’s Institute for CyberScience (ICS). For complete biographical information, please see the corresponding endnote.

^{**}**Amy C. Gaudion** is the Associate Dean for Academic Affairs & International Programs and assistant professor at Penn State’s Dickinson Law. For complete biographical information, please see the corresponding endnote.

^{***}**Jenni L. Evans** is the President of the American Meteorological Society, the Director of The Pennsylvania State University’s Institute for CyberScience, and a Professor of Meteorology at Penn State. For complete biographical information, please see the corresponding endnote.

satellites and smart devices, and we examine how the satellite-smart device information nexus works. We also address how private industry's aggregation of data through this nexus poses a threat to individual privacy, civil liberties, and national security.

In so doing, we work to fill a marked gap in the privacy and cyber-related legal literature when it comes to analyzing the technology, surveillance capabilities, law, and regulation behind government and commercial satellites *together* with private industry's aggregation, use, and dissemination of geolocation and other data from the satellite-smart device information nexus. This lack of awareness about the satellite-smart device information nexus has adverse consequences on individual privacy, civil liberties, and the security of nation states; it impedes informed legislation; and it leaves courts in the dark.

A contributing factor to the lack of awareness is that commercial remote sensing and government satellites are regulated by a byzantine scheme of international laws, treaties, organizations, and domestic nation states' laws that combine to control access to satellite data, sharing of satellite data, licensing, ownership, positioning in space, technical requirements, technical restrictions, and liability for harm caused by satellites. Although the satellite-smart device information nexus involves staggering quantities of personal information, we examine how the nexus falls outside the U.S. electronic surveillance and data legislative scheme and why it is unimpeded by privacy decisions due to a disconnect in U.S. Supreme Court decisions treating aerial surveillance differently than location tracking.

We breakdown the complex yet opaque regulatory structure governing commercial remote sensing and government satellites. We examine why the Strava event and others like it are—and will continue to be—the new norm, absent significant legislative and regulatory change. We conclude by providing a suggested roadmap for that legislative and regulatory change.

Table of Contents

I.	INTRODUCTION	594
II.	ARTICLE STRUCTURE AND TERMINOLOGY	596
	A. Overview of Article Structure	596
	B. Terminology	597
III.	SATELLITES: TECHNOLOGY AND INDUSTRY	603
	A. Satellites and Remote Sensing	604
	B. GNSS and U.S. GPS	606
	C. The Commercial Remote Sensing Industry and Its Use of Satellite Data	611
IV.	SMART DEVICES	615
	A. Smart Devices and GPS Receivers	616
	B. Sensor-based Information Systems	616
	C. Software Applications	621
V.	CASE STUDY: PRIVATE SECTOR AGGREGATION OF COMMERCIAL REMOTE SENSING, GPS, AND SENSOR DATA - THE STRAVA HEATMAP	622
VI.	SATELLITES AND REMOTE SENSING: LEGAL AND REGULATORY FRAMEWORK	625
	A. International Law and Regulation	625
	B. Regulation of U.S. GPS System	626
	C. U.S. Regulation of Commercial Remote Sensing	627
VII.	SATELLITES AND SMART DEVICES: U.S. LAW AND PRIVACY CONCERNS	631
	A. Constitutional Concepts of Privacy	633
	B. The Fourth Amendment and a Disconnect in Aerial Surveillance/Location Tracking Jurisprudence	634
	C. The U.S. Electronic Surveillance Statutory and Data Scheme	636
	D. Privacy and Civil Liberty Concerns	639
VIII.	SATELLITE DATA AND SMART DEVICES: NATIONAL SECURITY CONCERNS	640
	A. The Strava Heatmap: Understanding the National Security Impacts from the Aggregation of Remote Sensing Data and Smart Devices	642
	B. A Data Surprise: Why the U.S. Missed the Data Aggregation Threat	644
	1. Focusing on Other Threats to Satellites	644
	2. A Disjointed and Cumbersome Regulatory Regime	646
	C. The Limits of the Current Regulations and New Developments	651
	D. Data Aggregation Is a Persistent and Growing Concern	655
IX.	RECOMMENDATIONS	656
X.	CONCLUSION	663

I. INTRODUCTION



A Fitbit did that? On January 27, 2018, 20-year old Australian international security student Nathan Ruser tweeted: “Strava released their global heatmap. 13 trillion GPS points from their users . . . It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable.”¹

Instantaneously, Strava, a social media platform and mobile fitness app that works with wearable fitness devices, unintentionally compromised numerous U.S. special ops bases around the world by posting its “heatmap” of user activity online. Strava’s heavily-marketed heatmap comprises aggregated data of user movement, developed by synthesizing GPS satellite data for the movement data with satellite imagery to give these data a geographic reference.²

On January 30, 2018, *The New York Times* published a short video about Ruser’s tweet; it showed with startling clarity how satellite images combined with Strava’s heatmap data revealed multiple U.S. special ops bases in remote locations in Djibouti, Afghanistan, and Niger.³ *The Times* interviewed Ruser, who mused from his summer vacation in Thailand,

1. Nathan Ruser (@Nrg8000), TWITTER (Jan. 27, 2018, 10:24 AM), <https://twitter.com/Nrg8000/status/957318498102865920>.

2. See Drew Robb, *Building the Global Heatmap*, MEDIUM (Nov. 1, 2017), <https://medium.com/Strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de>.

3. Chritiaan Tribert et al., *How Strava’s Heat Map Uncovers Military Bases*, N.Y. TIMES, <https://nyti.ms/2DAjwxK> (last visited June 20, 2019).

“Whoever thought that operational security could be wrecked by a Fitbit?”⁴ The U.S. Department of Defense (DOD) was left scrambling, and the national security and privacy law communities were saucer-eyed with dawning comprehension. A social media fitness app simply was not on the Pentagon’s radar.⁵

To be clear: it is not our intent to imply that Strava did anything unlawful or violated its own terms of use and privacy policies. It did not. Moreover, Strava provides its users clear options to turn off data sharing. But the Strava reveal was a national security debacle and flagged significant privacy and civil liberty concerns. How did it happen? We explain the data aggregation behind Strava’s heatmap and explain why the Strava event is the new norm.⁶ Smart devices, software applications, and social media platforms – like Strava – routinely aggregate consumer data from multiple data collection sources, including device-embedded sensors, cameras, facial recognition software, and GPS, as well as from consumer activities like social media posts, pictures, texts, email, and contacts. These devices and apps utilize satellite data, including GPS, as a fundamental component of their data collection arsenal. This across-device, across-platform, and multi-sourced data aggregation is not being done by malicious actors, but rather by private industry. Nevertheless, the non-malicious aggregation of data poses a threat to individual privacy, civil liberties, and national security.

Law review articles abound that analyze the legal frameworks, ethical complexities, and technical know-how behind smart devices, software apps, and social media platforms and their data collection, aggregation, use, and sale. Likewise, a multitude of articles addressing privacy concerns and privacy-law based challenges to satellite-based mapping platforms, like Google Earth. However, there is a marked gap in the privacy and cyber-related legal literature when it comes to analyzing the technology, surveillance capabilities, and law behind government and privately-owned satellites together with the role and use of satellites and satellite data by the private sector via smart devices and apps.

The two groups – satellite experts/satellite law scholars on the one hand and cyber technology experts/cyberlaw and privacy scholars on the other – tend to stay in their own lanes when it comes to analysis of societal

4. Isabella Kwai, *What He Did on His Summer Break: Exposed a Global Security Flaw*, N.Y. TIMES (Jan. 30, 2018), <https://nyti.ms/2vpTfhh>.

5. Pun intended.

6. Cf. Ryan Pickrell, *Satellite Photos Reveal A Strategic Russian Military Upgrade on NATO’s Doorstep*, TASK & PURPOSE (Oct. 18, 2018, 10:38 AM), <https://taskandpurpose.com/russian-military-buildup-kaliningrad> (describing the use of satellite imagery to detect Russian military activity); SHAPE Public Affairs Office, *NATO releases satellite imagery showing Russian combat troops inside Ukraine*, NATO NEWSROOM (Nov. 26, 2014, 6:14 PM) <https://bit.ly/2L7RjVe> (same).

and security consequences flowing from acquisition, aggregation, and use of data from smart devices, apps, *and* satellites. Satellites are “up there” and governed by space and communications law, while “down-here” earth-based activities are governed by domestic legal authorities in the fields of surveillance, national security and privacy.

This gap in interdisciplinary scholarship has significant adverse consequences on an unaware public and the security of nation states. The Strava debacle made that abundantly clear. Privacy law scholarship has not comprehensively addressed questions like: How is government-owned satellite data made available to private entities? Who can own satellites? Who can access satellite data? How is it that a start-up using aggregated data from commercial, publicly available sources, such as satellite data, users’ smart devices, and software apps, can create a national security crisis overnight? To complicate matters, commercial and government satellites are regulated by a byzantine scheme of international laws, treaties, organizations, and domestic nation states’ laws that combine to control access to satellite data, sharing of satellite data, licensing, ownership, positioning in space, technical requirements, technical restrictions, and liability for harm caused by satellites. With few exceptions, scholarship addressing the law’s regulation of satellites and satellite data tends to fall squarely in either the traditional communications and space law camp or within technical and privacy scholarship regarding satellite technology, capabilities, and advances in these areas.

II. ARTICLE STRUCTURE AND TERMINOLOGY

A. *Overview of Article Structure*

This interdisciplinary paper begins to fill this void in the scholarship and is structured as follows.

In Section II(B), we address confusion caused by terminology and provide a list of defined terms as used in this article.

In Section III, we provide an overview of the technical capabilities of satellites, explain the basics of global position systems (GPS) satellite technology, and examine how the private sector uses data derived from and generated by commercial remote sensing satellite systems.

In Section IV, we analyze how smart devices, wearables, apps, social media platforms (like Strava), and wireless communications operate off the backbone of GPS receivers, microelectromechanical sensors, and satellite data. We explore how the private sector harnesses this satellite-device-software information nexus in ways not fully appreciated by the public or policymakers.

In Section V, we provide a case study, using the Strava heatmap, to demonstrate private sector use of commercial remote sensing and GPS and sensor data.

In Section VI, we provide an overview of the legal and regulatory frameworks, at the international and domestic levels, that govern space law, satellites, GPS, and the commercial remote sensing industry.

In Section VII, we provide a summary of the U.S. legal landscape governing electronic surveillance technologies, and we consider smart devices and satellite-generated and satellite-derived data in the context of privacy law, including constitutional concepts and Supreme Court jurisprudence. Finally, we assess the significant privacy and civil liberty challenges posed by the proliferation of smart devices, apps, and online communication platforms when combined with satellite data.

In Section VIII, we describe and analyze the specific threats to U.S. national security posed by the aggregation of satellite-generated data by private sector companies. We explore how and why the U.S. national security establishment failed to anticipate these threats, despite a slew of regulations that permit the U.S. government to restrict the collection, use, and dissemination of satellite data. We examine the shortcomings in the current regulatory regime, and we preview pending developments in the law. Finally, we explain that the Strava event was only a harbinger of a persistent and growing threat.

In Section IX, we propose a set of recommendations in broad brushstrokes to bridge the legal and regulatory chasms in this area while grappling with the powerful and transformative role that data from remote sensing satellites plays in our daily endeavors.

B. Terminology⁷

In an article tackling technical subjects like satellites, smart devices, embedded sensors, and data aggregation from a legal standpoint, our research spanned a wide array of research sources and revealed a confusing hodge-podge of terminology. The varying terms used by engineers, legislators, reporters, legal scholars, technical experts, and attorneys – in many cases to describe or refer to the exact same thing – leads to continued confusion, lack of understanding, and separation of knowledge and disciplines. The term “GPS satellite data,” for example, is alternatively referred to as geospatial data, digital geolocation data, geodata, GPS, satellite location data, and remote sensing data.

7. The authors gratefully wish to acknowledge the research and citation assistance with this terminology section provided by Benjamin L. Cohen, J.D., Penn State Dickinson Law, and Wyatt C. Weisenberg, J.D. Candidate, Penn State Dickinson Law, J.D. anticipated May 2020.

To alleviate this confusion, the following terms are defined as follows:

5th Generation Wireless (5G) is a new form of wireless networking technology which promises download speeds approximately 20 times faster than the current 4th Generation (4G) technology. Previously, wireless networking operated using the radio-frequency spectrum. 5G marks a shift away from the radio-frequency spectrum to the millimeter wave spectrum. Unlike the radio waves of prior generations, millimeter waves cannot easily transmit through obstacles. 5G wireless thus requires a denser number of cell sites. 5G's denser network of cell sites allows increased transmission speeds. 5G simultaneously relies on a traffic-signaling system to identify the most efficient delivery route. The new cell sites transmit information simultaneously across the same frequency. This transmission principle can potentially double the capacity of wireless networks at their most fundamental physical layer.⁸

Cellular phones are two-way telecommunication devices that are perhaps best understood as sophisticated radios.⁹ The root "cell" in cellular refers to geographic regions often illustrated as hexagons, like that of a bee's honeycomb.¹⁰ Cellular phones contain a low-power transmitter that transmits and receives information through a network of cell sites.¹¹ Cell phones scan for the cell site that offers the strongest signal in its geographic area.¹² The cell phone performs these scans every seven seconds or when the signal strength from one cell site or tower weakens, regardless of whether a call is placed.¹³

Cell sites, also referred to as *cell towers*, sit along areas where three hexagonal cells connect.¹⁴ Each cell site or cell tower contains a radio transceiver and base station controller that receives and transmit verbal

8. See Charlotte Lee, *The 5G Economy: How 5G will Impact Global Industries, The Economy, and You*, MIT TECHNOLOGY REVIEW (Mar. 1, 2017), <https://bit.ly/2o9T9V1>; see also Amy Nordrum et al., *Everything You Need to Know About 5G*, IEEE SPECTRUM BLOG (Jan. 27, 2017, 7:00 PM), <https://bit.ly/2OV1Dhh>.

9. CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 28:2 (3d ed. Supp. 2018), Westlaw WIRETAP; see also *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 750–751 (S.D. Tex. 2005). For a general background on cellular telephones, see S. REP. NO. 99-541 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3563.

10. See *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d at 750 (describing cellular phone technology).

11. See *id.*

12. *Id.*

13. *Id.*

14. *Id.*

communications from one cellular phone to another.¹⁵ Cell sites do not only process voice data; cell sites also receive location data.

Cell Site Location Information (CSLI) is a time-stamped record of cell phone's location that is generated each time a cellular phone scans or connects to a cell site.¹⁶ As noted, cell phones continuously scan for nearby cell sites. Cell phones connect to the cell site when placing a phone call, sending text messages, and when using a cellular phone application.¹⁷ While the accuracy of the CSLI varies dependent upon the concentration of cell sites within a given area, the ubiquity of cellular phones results in an increasingly compact coverage areas, and thereby an increasingly accurate CSLI.¹⁸ With the proliferation of smart phones, mobile apps and texting communication platforms, "modern cell phones generate increasingly vast amounts of increasingly precise CSLI."¹⁹ The accuracy of CSLI is further compounded by the commercialization of location data CSLI, incentivizing the cellular providers to store CSLI beyond that required by law.²⁰

Cellular tracking is a surveillance method that uses CSLI to determine real-time movement and historical movement (over time) by comparing the difference in signal strength from multiple different cell sites.²¹ This process is also known as *cellular triangulation* and is distinct from *geolocation tracking*, which is defined below.

Geolocation data refers to digital geographic data and information concerning objects or phenomena that are directly or indirectly associated with a location relative to the Earth.²² Geolocation data reflects the geographical (latitudinal and longitudinal) location of an Internet-connected device or GPS receiver enabled device.²³ Geolocation data collected from such devices is used, accessed, and disseminated by a variety of apps, and even other smart devices.²⁴ The geolocation data

15. *Id.*

16. *See* *Carpenter v. United States*, 138 S. Ct. 2206, 2211–12 (2018).

17. *See id.* at 2212.

18. *Id.*

19. *Id.* at 2212.

20. *See generally id.* (noting that wireless carriers often sell aggregated location records); *Enhanced 911 – Wireless Services*, FED. COMM'NS COMM'N, <https://www.fcc.gov/general/enhanced-9-1-1-wireless-services> (last visited June 20, 2019) (requiring cell network providers be able to provide relatively precise locations of persons placing 911 calls from mobile devices)

21. *See* Aaron Blank, *The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone*, 18 RICH. J.L. & TECH. 3, 7–10; *see also* FISHMAN & MCKENNA, *supra* note 9, § 28:4.

22. *Geolocating Carmen Sandiego*, GRAVITATE (Dec. 14, 2018), <https://www.gravitatedesign.com/blog/what-is-geolocation/>.

23. *Id.*

24. *Id.*

collected reflects the geolocation of the device or server, in other words, “if you leave your phone in your car and go for an hour-long run in silence . . . , your geolocation history for that hour is the physical location of your car (according to your phone).”²⁵ In contrast, if “your fitness tracker traveled with you the whole time on your wrist, its geolocation history for that hour is wherever you ran.”²⁶ Of course, if your phone is synced with your fitness tracker or other wearable device, your phone will collect the geolocation data from the fitness tracker when the two devices next connect.

Geolocation tracking is a surveillance method similar to *cellular tracking* but relies on GPS satellite data captured and stored by GPS receivers, rather than cell-site location data. Geolocation tracking relies on a trilateration process, as opposed to triangulation.²⁷

Geospatial data is data that has a geographic component or includes locational information, such as geographic data in the form of coordinates, address, city, or ZIP code. Geospatial data can originate from GPS data, satellite imagery, and geotagging.²⁸ Geospatial data may also be referred to as location data or spatial data and is emerging as an important source of information both in traditional and in big data analytics.²⁹

Geospatial technology refers to the technology used to “acquire, manipulate, and store geographic information.”³⁰ Examples of geospatial technologies include GPS and remote sensing, among others.³¹

GPS satellite data means electronic information about the time and position of a GPS satellite.³²

GPS chips or GPS receivers are computer processors that receive GPS signals from satellites to determine the device’s geolocation. Devices with a GPS chip typically have wireless connectivity which enables the device to transmit data to a secondary device, such as a personal computer or mobile phone.³³

25. *Id.*

26. *Id.*

27. Daniel Ionescu, *Geolocation 101: How It Works, the Apps, and Your Privacy*, PCWORLD (Mar. 29, 2010), <https://www.peworld.com/article/192803/geolo.html>.

28. Caitlin Dempsey, *What is the Difference Between GIS and Geospatial?*, GIS LOUNGE (Jan. 14, 2014), <https://www.gislounge.com/difference-gis-geospatial/>.

29. *Id.*

30. *Id.*

31. *Id.*

32. *See What is WAAS?*, GARMIN, <https://www8.garmin.com/aboutGPS/waas.html> (last visited June 20, 2019).

33. *See* Amanda Thomas, *How Micro GPS Tracking Chips Work*, TRACKIMO (Jul. 26, 2016), <https://trackimo.com/micro-gps-tracking-chips/>; *see also* Daniel Rubino, *GPS vs.*

Assisted-GPS or *aGPS* is the combined use of GPS along with Wi-Fi and cell-tower triangulation (see definition below) to pinpoint the location of a device.³⁴ Assisted-GPS pinpoints location very accurately, especially indoors where GPS signals might not be strong.³⁵

Internet of Things (IoT) refers to a decentralized network of embedded sensors and processors, enabling a range of possible communications: person-to-device, device-to-device, or device-to-grid. These systems monitor and manage *IoT devices*.³⁶

IoT devices are physical objects capable of connecting to the internet, similar to other smart devices, with a stronger emphasis on *device-to-grid* communications to enable data analytics.³⁷

Remote sensing is a method of data collection through instruments or sensors that act as a proxy to direct forms of information that rely on physical contact.³⁸

Commercial remote sensing space capabilities as defined in the U.S. Commercial Remote Sensing Policy “refers to privately owned and operated space systems licensed under the Land Remote Sensing Policy Act of 1992, their technology, components, products, data, services, and related information, as well as foreign systems whose products and services are sold commercially.”³⁹

Remote sensing space capabilities are similarly defined in the Policy as “all remote sensing space systems, technology, components, products, data, services, and related information.”⁴⁰ Space systems include the spacecraft’s remote sensing hardware, software, and cargo as well as the spacecraft’s ground stations, command facilities, and the connecting networks. Data processing components and exploitation hardware and

aGPS: A Quick Tutorial, WINDOWS CENTRAL (Jan. 3, 2009), <https://www.windowcentral.com/gps-vs-agps-quick-tutorial>.

34. See Tracy V. Wilson, *How GPS Phones Work*, HOWSTUFFWORKS, <https://bit.ly/2HdZvze> (last visited on June 20, 2019).

35. See Jules G. McNeff, *The Global Positioning System*, 50 IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECH. 645, 646–647 (2003), <https://bit.ly/2VpS5Rq>.

36. See MCKINSEY GLOBAL INSTITUTE, *THE INTERNET OF THINGS: MAPPING THE VALUE BEYOND THE HYPE* 17 (2015), <https://mck.co/2gyPezB>; see also THE HAMMERSMITH GROUP, *INTERNET OF THINGS: NETWORKED OBJECTS AND SMART DEVICES*, (2010), <https://bit.ly/2UXcA8u>.

37. See Mayank Singh, *Smart, Connected and IoT Device*, ENGINEERING ECKOVATION (Jun. 6, 2018), <https://engineering.eckovation.com/smart-connected-iot-devices/>.

38. See 15 C.F.R. § 966.3 (2018) (defining remoting sensing system as applied to satellites); 51 U.S.C. § 60101(4) (defining land remote sensing).

39. NAT’L OCEANIC & ATMOSPHERIC ADMIN., U.S. COMMERCIAL REMOTE SENSING POLICY FACT SHEET 1 (April 25, 2003), <https://bit.ly/2VzywpC> [hereinafter REMOTE SENSING POLICY].

40. *Id.*

software with remote sensing characteristics may also be included in the definition.⁴¹

Smart or *smart devices* are physical objects capable of connecting to the internet, either directly or indirectly through a network, to communicate information with other networked devices; and have computer processing capabilities for collecting, sending, receiving, or analyzing data.⁴² *Smart* has now colloquially become a prefix used to modify a word, signaling that the modified word has some form of networking and processing capabilities. Put differently, *smart* + *X* refers to *X* with the ability of networking and computer processing. For example, *smartcity* refers to a city that has incorporated networking and computer processing technology into its urban environment.

Smartphones refer to mobile or cellular phones embedded with high-performance microprocessors and other sensors powered by a mobile operating system featuring capabilities like a traditional computer.⁴³

Software applications, or *apps*, are software programs that function on top of a device's operating system, allowing the user to perform all sorts of tasks from editing documents to playing games. Applications have been around for as long as computers, but the term 'app' is associated with the software that runs on a smartphone or tablet device.⁴⁴

Triangulation is the process of determining the coordinates of a point based on the known location of two other points. If the direction (but not distance) from each known point to the unknown point can be determined, then a triangle can be drawn connecting all three points. While only the length of one side of the triangle is known at first (the side connecting the two known points), simple trigonometry reveals the lengths of the other sides and so the position of the third point. In the context of cell site information, the two known points are the antenna towers, the third point is the cellular telephone, and the direction from each tower to the phone is

41. *Id.*

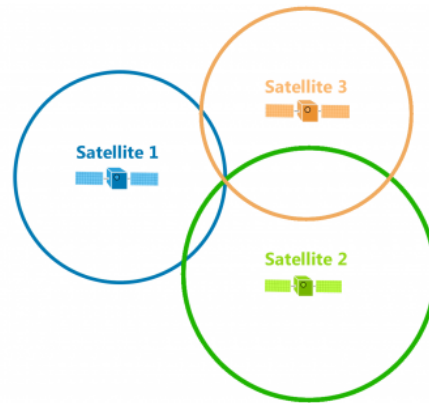
42. See Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S. 1691, 115th Cong. § 2 (2017); SMART IoT Act, H.R. 6032, 115th Cong. § 2 (2017); S.B. 327, 2017 Leg. (Cal. 2018).

43. See *What is a smartphone?*, LENOVO, <https://lnv.gy/2WAIPar> (last visited June 20, 2019).

44. See Marziah Karch, *A Beginner's Guide to Apps*, LIFEWIRE, (last updated Jan. 04, 2019), <https://bit.ly/2HbzNeK>; *What is an app?*, BBC WEBWISE BLOG, <http://www.bbc.co.uk/webwise/0/27488178> (last updated Jun. 2, 2014, 2:26 PM); *Understanding Mobile Apps*, FED. TRADE COMM'N, <https://bit.ly/28KjSIG> (last visited June 20, 2019).

discerned from the information about which face of each tower is facing the phone.⁴⁵

Trilateration is the process of determining the position of a point based on the known location and known distance to three other points. When a GPS device receives a signal from a satellite, the system calculates the distance between the receiver and the satellite, identifying the possible position of the device as anywhere within the satellite's signal radius. This process repeats with another satellite. With two signals, the precise position could be any of the two points where the two circles of signal coverage intersect. This is still not precise enough, leading to a third satellite joining the process, revealing the device's precise location



where all three circles intersect. Each satellite is at the center of a sphere with the GPS receiver found in the location where the satellites intersect.⁴⁶

Wearable devices describe physical objects such as fitness trackers, smartwatches, or smart glasses worn by the user with embedded or integrated processors and sensors that are typically networked to a mobile device, offering consumers and businesses access to real-time, highly personalized information.⁴⁷

III. SATELLITES: TECHNOLOGY AND INDUSTRY

*The possibility of integrating remote sensing data into local...databases and using the databases in conjunction with locational GPS data has created opportunities for new types of information applications that were not possible using photographic remote sensing data alone.*⁴⁸

45. See FISHMAN & MCKENNA, *supra* note 9, at § 28:4; see also *Trilateration vs Triangulation – How GPS Receivers Work*, GIS GEOGRAPHY, <https://bit.ly/2Q0kfgz> (last updated Mar. 4, 2019).

46. *Trilateration vs Triangulation – How GPS Receivers Work*, GIS GEOGRAPHY, <https://bit.ly/2Q0kfgz> (last updated Mar. 4, 2019).

47. Disrupter Series: Wearable Devices: Hearing Before the Subcomm. on Commerce, Mfg., and Trade, Comm. on Energy and Commerce, 114th Cong. 2–3 (2016) (statement of Hon. Michael C. Burgess, Rep. from Tex.), <https://bit.ly/2WwbhtY>.

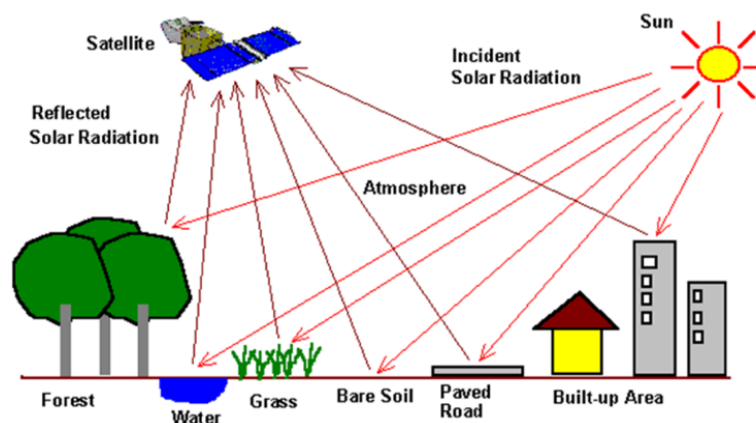
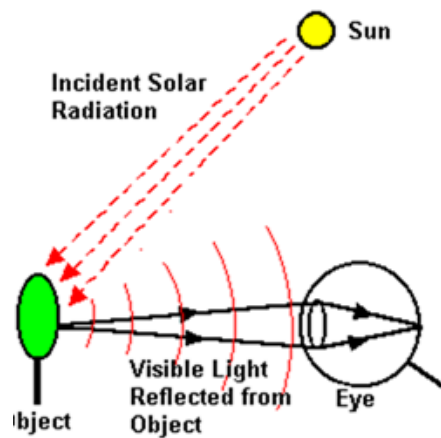
48. NAT'L RESEARCH COUNCIL, *USING REMOTE SENSING IN STATE AND LOCAL GOVERNMENT: INFORMATION FOR MANAGEMENT AND DECISION MAKING* 17 (Nat'l Academies Press 2003).

After the January 2018 Strava reveal, this 2003 statement from a National Research Council report proves prescient. The posting of the Strava heatmap, with its immediate national security impact, demonstrates this application of locational GPS data from the smart devices onto satellite-derived topography and land use backgrounds. This section provides a basic overview of the technical capabilities of satellites, examines how the private sector uses data generated from commercial remote sensing satellite systems, and overviews global positioning system (GPS) capabilities.

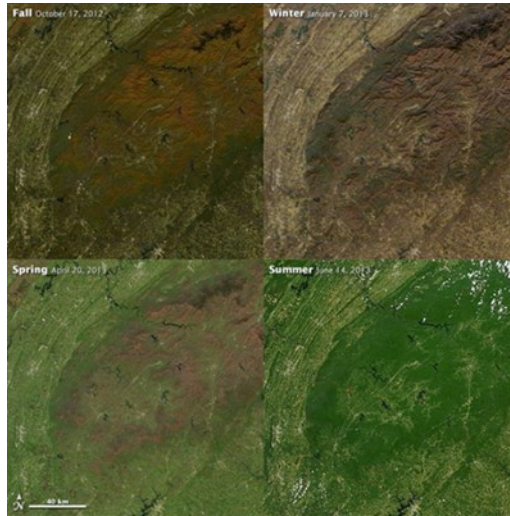
A. *Satellites and Remote Sensing*

Satellites work in a similar way to the human eye. Neither receives information about an entire object; they sense the presence (or absence) of a feature remotely. Touch is direct sensing – you are in physical contact with the object. Remote sensing is the process of acquiring information about your surroundings *without* being in contact with it. Both the eye and the Earth-orbiting satellite sense reflected or emitted energy, then process and interpret that data into usable information about the world around us.

Satellites carry a variety of instruments to capture different parts of the energy spectrum, including visible (what you see is what you get),



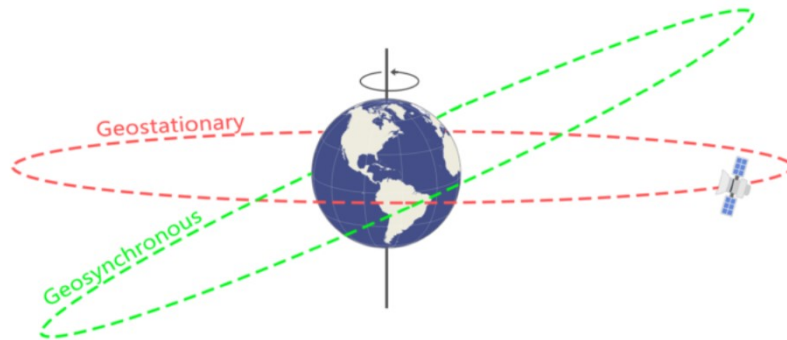
infrared (temperature), and microwave (clouds, rain, ice, snow) parts of the spectrum. Using data from more than one of these sensors in combination empowers us to distinguish between various types of clouds and weather systems, different types of land cover (ploughed fields, grasslands, cities, forests, lakes, ocean), and topography. The end result of this process is given in the Landsat example to the right.⁴⁹ These four merged images are developed by combining information from many satellite retrievals of the Smoky Mountains in each season over 2012 and 2013 and capture seasonal differences in vegetation and other features. In broad terms, this is the process for visualizing land surface information, such as that in the Strava images.



Aggregation of satellite data by commercial entities includes data from satellites in orbits categorized as geostationary, geosynchronous, and semi-synchronous. Geostationary satellites orbit above the equator in high Earth orbit at an altitude of roughly 36,000 kilometers. This high altitude is necessary for the satellite to “sit” in a constant relative location above the Earth’s surface and allows the satellite to lie on the same plane as the equator. The advantages of geostationary satellites are constant and consistent views of the same areas. The disadvantage is that the resolution of the satellite is diminished by distance. Geostationary satellites are generally used for weather monitoring, and search and rescue beacons.⁵⁰

49. Holli Riebeck, *How to Interpret a Satellite Image: Five Tips and Strategies*, NASA EARTH OBSERVATORY (2013), <https://earthobservatory.nasa.gov/features/ColorImage>.

50. *Geosynchronous vs Geostationary Orbits*, GIS GEOGRAPHY (Feb. 23, 2018), <https://gisgeography.com/geosynchronous-geostationary-orbits/>.



51

Geosynchronous satellites are located in “a sweet spot above the Earth” where the satellite is able to match the Earth’s rotation.⁵² Thus, a geosynchronous satellite’s orbit synchronizes with the rotation of the Earth, and it matches the time it takes for the Earth to rotate on its axis - 23 hours, 56 minutes and 4.09 seconds.⁵³ Geosynchronous satellites move in a constant low-Earth orbit, with an altitude of roughly 350 kilometers.⁵⁴ The low orbit and proximity to the Earth’s surface allows for higher resolution images, and makes geosynchronous satellites particularly useful for telecommunications and other remote sensing applications.⁵⁵

Semi-synchronous satellites orbit in a medium Earth orbit located approximately 20,200 kilometers above the surface of the planet. Satellites in semi-synchronous orbit take approximately 12 hours to complete an orbit, twice as fast as the 24-hour cycle for geosynchronous satellites. These semi-synchronous satellites make up the global position systems (GPS) satellites systems that are critical to the aggregation of locational data.

B. GNSS and U.S. GPS

To understand how private industries typically interact with satellites and satellite data, it is helpful to understand the basics of GPS satellite

51. *Id.*

52. *Id.*

53. *Id.*

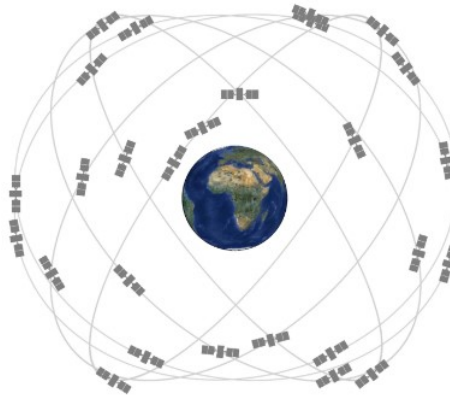
54. *Id.*

55. *Id.*

technology as GPS is one of the most commercially common uses of satellites. Before we further describe GPS satellite technology, it is important to remember that the Strava debacle was not caused only by Strava's interaction with satellites, but also by Strava's users' interaction with satellites. This begs the question: how do individuals interact with satellites and satellite data? To help answer this question, meet Corey, a U.S. citizen residing in the U.S. Like many Americans, Corey uses a smartphone and a wearable fitness device. Corey does not exist, but Corey does represent the average person. Corey could be you; Corey could be me. For illustrative purposes, imagine Corey just purchased the newest iPhone. Corey inputs Corey's home address into the phone's navigation application and begins the journey home. The U.S. GPS system and Corey's smart devices go to work to get Corey home. To understand how this happens, we turn back to the satellite systems at play here. What is GPS and how does work?

The Global Navigation Satellite System (GNSS) is the standard generic term for satellite navigation systems that provide autonomous geospatial positioning with global coverage.⁵⁶ GNSS is a term used worldwide, and sometimes used interchangeably with the term GPS (Global Positioning System). As discussed more fully below, the major GNSS Systems are GPS (U.S.), GLONASS (Russia), Galileo (European Union), BeiDou (China), and other regional systems.⁵⁷

The U.S. GPS is a satellite-based navigation system owned and developed by the U.S. Government. The U.S. GPS constellation consists of 31 operational satellites out of which 24 are active at any given time to cover at least 95% of the earth.⁵⁸ The satellites fly in medium Earth orbit at an altitude of approximately 20,200 kilometers,⁵⁹ as



56. Michael Venezia, *What is the Difference Between GNSS and GPS?*, SYMMETRY ELECTRONICS (Dec. 16, 2015), <https://www.semiconductorstore.com/blog/2015/What-is-the-Difference-Between-GNSS-and-GPS/1550/>.

57. *Id.* Access to multiple satellites increases accuracy, redundancy and availability at all times; and if one GNSS system fails, GNSS receivers can pick up signals from other systems.

58. *Space Segment*, GPS.GOV, <https://www.gps.gov/systems/gps/space/> (last updated Mar. 21, 2019). For more info on technical aspects of the GNSS, see *Technical Documentation*, GPS.GOV, <https://www.gps.gov/technical/> (last updated Sept. 5, 2018).

59. *Id.*

depicted in the diagram of the U.S. GPS constellation.⁶⁰ The U.S. Air Force is responsible for the GPS satellites, and expects to launch its next GPS satellite in July 2019.

GPS satellites are placed into orbits in such a way that any point on earth is in the direct line of sight of at least four satellites. GPS satellites broadcast radio signals that contain the time and then location of the GPS satellites.⁶¹ GPS receivers are “chips” that can read the signals that GPS satellites broadcast.⁶² These receiver chips essentially read the digital radio signals at the frequency in which the satellites broadcast the digital signals.⁶³ GPS receivers read the radio signals from any four satellites from which the GPS receiver gets a signal, and then doing some computations, the GPS receiver infers its own or its device’s position using trilateration.⁶⁴ Thus, the GPS satellites, apart from broadcasting their own location, do not take part in the process of gathering geolocation data or geolocation tracking.⁶⁵

Fortunately for Corey (or for Apple, the manufacturer of Corey’s iPhone), civilian use of the U.S. GPS satellite system is free. Because use of U.S. GPS is free, numerous private companies develop chips compatible with U.S. GPS.⁶⁶

How does a smart device use GPS? Recall that Corey is using a smartphone to determine directions home. Corey inputs the address into a navigation application used by the smart phone. The navigation app uses information collected from the GPS chip in the phone to provide Corey with the fastest route home.⁶⁷ The phone’s GPS chip receives digital radio signals at the frequency in which the satellites broadcast the digital signals,

60. *Id.*

61. GPS satellites have atomic clock in them that allow the satellites to keep very accurate time and these clocks are adjusted daily to maintain unanimity with time on earth. GPS satellites have a decided orbit and it is easy to know their location at any given time. *Id.*

62. Patrick Bertagna, *How Does a GPS Tracking System Work?*, EE TIMES (Oct. 26, 2010), https://www.eetimes.com/document.asp?doc_id=1278363.

63. *Id.*

64. Marshall Brain & Tom Harris, *How GPS Receivers Work*, HOWSTUFFWORKS 1, <https://electronics.howstuffworks.com/gadgets/travel/gps.htm> (last visited June 20, 2019). Specifically, for a discussion of trilateration, see *id.* at 3, <https://electronics.howstuffworks.com/gadgets/travel/gps2.htm>.

65. Wilson, *supra* note 34.

66. Sarah Laskov, *The Plane Crash That Gave Americans GPS*, THE ATLANTIC (Nov. 3, 2014), <https://www.theatlantic.com/technology/archive/2014/11/the-plane-crash-that-gave-americans-gps/382204/>.

67. See Manisha Priyadarshini, *Which Sensors Do I Have In My Smartphone? How Do They Work?*, FOSSBYTES (Sept. 25, 2018), <https://fossbytes.com/which-smartphone-sensors-how-work/>.

allowing the application to gather relevant time and location data from the digital signals.⁶⁸

As GPS satellites do not actively participate in location gathering but passively broadcast signals for everyone and anyone to read, billions of mobile devices and other GPS-chip embedded devices are able to use GPS simultaneously.⁶⁹ Recall the assisted-GPS discussion above. When a mobile app is in use, the app is able to utilize assisted-GPS, which is GPS receiver chip data in conjunction with Wi-Fi and cell-tower triangulation, to precisely pinpoint the location of the device.⁷⁰ Assisted-GPS pinpoints location with precise physical accuracy, especially indoors where GPS signals might not be strong.

As noted, GPS is a system owned and operated by the U.S. Government, and the U.S. can selectively decide to deny any nation access to GPS data.⁷¹ While GPS was initially developed by and for the U.S. military, free, worldwide use for civilians was enabled in 1983.⁷² Initially, the U.S. scrambled the signal to limit GPS accuracy for national security purposes, but the result was that the U.S. GPS satellites were too inaccurate for viable use in everyday commercial activities. In 2000, President Clinton made the unscrambled signal available to the public.⁷³

The U.S. GPS broadcasts in L1 through L5 frequencies.⁷⁴ Of these, the L1 and L5 can be used for civilian purposes whereas the L2 has some frequencies dedicated to military use.⁷⁵ L2 is encrypted and only a device with the correct decryption key can access that code.⁷⁶ The L5 band is a newly added band that provides an internationally-protected range for

68. *See id.*

69. McNeff, *supra* note 33, at 646–47.

70. Wilson, *supra* note 34.

71. Ishan Srivastava, *How Kargil spurred India to design own GPS*, THE TIMES OF INDIA (Apr. 5, 2014), <https://timesofindia.indiatimes.com/home/science/How-Kargil-spurred-India-to-design-own-GPS/articleshow/33254691.cms>. The United States denied India access to the GPS satellites during the Kargil War in 1999 which led to India developing its own satellite system consisting of seven satellites that cover the entire landmass of India. *Id.*

72. Allegedly, the U.S. made its GPS satellites free and open to civilian use after Russia shot down a Korean civilian airliner that strayed from its flight path and entered Russian territory. *See* Mark Sullivan, *A Brief History of GPS*, PCWORLD (Aug. 9, 2012, 7:00 AM), <https://www.pcworld.com/article/2000276/a-brief-history-of-gps.html>.

73. Juquai McDuffie, *Why the Military Released GPS to the Public*, POPULAR MECHANICS (June 19, 2017), <https://www.popularmechanics.com/technology/gadgets/a26980/why-the-military-released-gps-to-the-public/>; *Clinton Acts to Make GPS More Accurate*, N.Y. TIMES (May 2, 2000), <https://www.nytimes.com/2000/05/02/technology/clinton-acts-to-make-gps-more-accurate.html>.

74. *New Civil Signals*, GPS.GOV, <https://www.gps.gov/systems/gps/modernization/civilsignals/> (last visited June 20, 2019).

75. *Id.*

76. *Id.*

aeronautical navigation, promising little or no interference under all circumstances.⁷⁷ In the early 2000s, GPS accuracy was about 20 feet; however, since the deployment of satellites using the L5 band, the accuracy is up to 12 inches.⁷⁸ New GPS receivers using this band can pinpoint location to within a foot, anywhere on earth.⁷⁹

Other countries also have GNSS systems or are rapidly developing and deploying their own GNSS GPS-like systems. Russia has GLONASS, a GNSS system with global coverage,⁸⁰ and the EU has Galileo. China has engaged in rapid development and deployment, launching 18 GPS satellites in 2018 alone, and France is also developing its own GNSS systems for worldwide coverage.⁸¹ The goal – independence from the U.S. monopoly on GPS. This December 2018 techcrunch.com research graph by Arman Tabatabai summarizes 2018 GPS satellite development and launch activity by major nation states.⁸²

Country	System Name	Satellites Deployed	Full Operational Date	2018 Launches	Cost?
USA	GPS	31 - 33	1978	—	\$12B
Russia	GLONASS	24 - 26	1995	2	\$4B - \$11B
EU	Galileo	26	2019-20	4	10B Euro
China	Beidou	35 - 40+	2020	18	\$8.98B - \$10.6B
Japan	QZSS	4	2018	—	170B Yen
India	IRNSS	7	—	1	\$313M
UK	Unconfirmed	—	—	—	Up to 5B GBP

Because the U.S. GPS was the first GNSS satellite system to be made available for free use by civilians worldwide, device-manufacturers in the U.S and elsewhere, including cellular and smart device manufacturers, developed GPS receiver chips that were compatible with the U.S. GPS satellites.

77. *Id.*

78. Samuel K. Moore, *Superaccurate GPS Chips Coming to Smartphones in 2018*, IEEE SPECTRUM (Sept. 21, 2017, 1:00 PM), <https://spectrum.ieee.org/tech-talk/semiconductors/design/superaccurate-gps-chips-coming-to-smartphones-in-2018>; Jacob Kastrenakes, *GPS will be Accurate within One Foot in some Phones Next Year*, THE VERGE (Sept. 25, 2017, 2:32 PM), <https://www.theverge.com/circuitbreaker/2017/9/25/16362296/gps-accuracy-improving-one-foot-broadcom>.

79. Moore, *supra* note 78.

80. Danny Crichton & Arman Tabatabai, *The GPS Wars have Begun*, TECHCRUNCH (Dec. 21, 2018), <https://techcrunch.com/2018/12/21/the-gps-wars-have-begun/>.

81. *Id.*

82. *Id.*

C. *The Commercial Remote Sensing Industry and Its Use of Satellite Data*

*Elevate your perspective. Don't speculate; quantify. Tap into the DigitalGlobe to extract insights and validate critical decisions. DigitalGlobe makes valuable location-based information accessible to those who need it—anywhere, anytime.*⁸³

That's one marketing tagline by DigitalGlobe, one of largest commercial remote sensing satellite owners and operators. Now that we understand how satellites work, this section summarizes the commercial remote sensing industry and describes how private companies collect and use satellite generated data. In the last few years, significant media and scholarly attention has focused on the use of unmanned aerial vehicles (UAVs), or drones by the both private sector and government. While UAVs provide a cheap and readily accessible means of aerial surveillance and data collection,⁸⁴ commercial entities have engaged in aerial data collection long before drones became part of our lexicon. Private companies have been capturing and commercializing satellite data and satellite images of our planet for decades.⁸⁵

In 1994, the U.S. government granted Lockheed Martin one of the first licenses for commercial satellite high-resolution imagery. With that license, the company developed IKONOS, the first commercial remote sensing system satellite.⁸⁶ Launched in 1999, it was the first commercial satellite to collect high-resolution imagery of the Earth, and to make it publicly available.⁸⁷ Since the 1999 launch of IKONOS, the number of commercial actors engaged in the remote sensing industry has expanded significantly. The commercial remote sensing services market is estimated to reach \$21.62 billion by 2022; that growth is being fueled by defense and

83. *Home*, DIGITALGLOBE, <https://www.digitalglobe.com/> (last visited June 20, 2019) (*italics added for emphasis*). (Taglines on DigitalGlobe's website change frequently. The above tagline appeared in April of 2019.)

84. *See, e.g.*, Stephen Rice, *Eyes In the Sky: The Public Has Privacy Concerns About Drones*, FORBES (Feb. 4, 2019, 10:00 AM), <https://bit.ly/2Hes5iU>; *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, ELEC. PRIVACY INFO. CTR., <https://epic.org/privacy/drones/> (last visited June 20, 2019); ANN CAVOUKIAN, INFO. & PRIVACY COMM'R OF ONT., *PRIVACY AND DRONES: UNMANNED AERIAL VEHICLES* (2012), <https://bit.ly/30cngz2>.

85. *See* Janna J. Lewis & Lauren R. Caplan, *Drones to Satellites, Should Commercial Aerial Data Collection Regulations Differ by Altitude?*, SCITECH LAWYER, Summer 2015, at 10, 10.

86. Christopher Lavers, *The Origins of High Resolution Civilian Satellite Imaging - Part 2: Civilian Imagery Programs and Providers*, DIRECTIONS MAGAZINE (Feb. 4, 2013), <https://www.directionsmag.com/article/1646>.

87. *Id.*

private sector use of remote sensing services, supported by satellites, as well as Big Data applications.⁸⁸

Two of the most significant commercial satellite players are DigitalGlobe and SPOT Image.⁸⁹ GeoEye was a third large player, but DigitalGlobe purchased GeoEye and all of its subsidiaries and satellites in 2013.⁹⁰ These commercial entities use their remote sensing satellites to collect various sorts of data, including images, location data, and real-time surveillance, and then sell that satellite data to both private sector and governments. But the raw satellite data is not the only commodity being sold. These companies also aggregate data and provide geospatial analysis of the satellite-generated data, and then sell that analysis to app developers, social media platforms and government entities. Several examples from the commercial remote sensing industry may prove helpful in appreciating the scale and scope of the data collection and use.



91

Let's start with DigitalGlobe. The montage above shows differing types of images and data captured by DigitalGlobe's various satellites. According to DigitalGlobe's 2018 brochure, its constellation of satellites

88. *Remote Sensing Services Market Will Worth \$21.62 Billion by 2022: Report*, GEOSPATIAL WORLD (Oct. 31, 2017), <https://www.geospatialworld.net/news/remote-sensing-services-market-will-worth-21-62-billion-2022-report/>.

89. *Id.*

90. *Private Remote Sensing System License Summary of GeoEye-1*, NAT'L OCEANIC & ATMOSPHERIC ADMIN. (Feb. 28, 2013), <https://www.nesdis.noaa.gov/CRSRA/files/GeoEye1.pdf>. [hereinafter *GeoEye-1 License*].

91. DIGITALGLOBE, THE DIGITALGLOBE CONSTELLATION (2018), https://dgv4-cms-production.s3.amazonaws.com/uploads/document/file/126/Constellation_Brochure_2018.pdf.

“collects more than one billion sq. kilometers of high-resolution imagery per year—building and refreshing the most comprehensive and up-to-date high-resolution imagery library in the world as well as offering tremendous tasking capacity.” The company explains, “You choose the world imagery you need and the way you need it—online, offline, on your mobile device or directly into your GIS—and we deliver real-world perspective you can rely on.”

DigitalGlobe’s constellation of satellites⁹² is noteworthy for several reasons. It was the first company to deliver imagery data at full—or 30 centimeter—resolution to its private sector customers.⁹³ Prior to 2015, the U.S. government was the only entity able to obtain full resolution data; all other entities received data subsampled down to 50 centimeters.⁹⁴ In 2015, that changed when the U.S. government “cleared” DigitalGlobe “to sell” these “clearer, richer”⁹⁵ images. Because its satellites move in constant low-Earth orbit, with an altitude of roughly 600 kilometers,⁹⁶ DigitalGlobe has the ability to capture and the advantage of being able to provide its customers much more detailed images of the Earth’s surface.

The second reason DigitalGlobe’s constellation of satellites is noteworthy is that the company is dominating the remote sensing market. In 2008, DigitalGlobe signed agreements with Google, Microsoft, Nokia and other customers to support their location-based services and mapping applications by providing access to DigitalGlobe’s high-resolution satellite imagery.⁹⁷ Look at almost any recent news article involving world events, including missile launches by North Korea⁹⁸ and California’s 2018 wildfires,⁹⁹ and the credit below the image will say “provided by DigitalGlobe.” In addition to government agencies and news organizations, customers for the DigitalGlobe satellite products include other commercial data providers, including Mapbox¹⁰⁰ and Google

92. For an overview of the entire system, see DIGITALGLOBE, *supra* note 91. In August 2014, DigitalGlobe launched WorldView-3, the company’s eighth satellite at the time. In the last five years, DigitalGlobe also launched WorldView-4.

93. See *About DigitalGlobe*, DIGITALGLOBE, <https://www.digitalglobe.com/company/about-us> (last visited June 20, 2019).

94. See DIGITALGLOBE, *supra* note 91.

95. *About DigitalGlobe*, *supra* note 93.

96. See Richard Hollingham, *Inside the Google Earth Satellite Factory*, BBC FUTURE (Feb. 11, 2014), <https://bbc.in/1eqRmxQ>.

97. See *About DigitalGlobe*, *supra* note 93.

98. See David Brunnstrom, *Satellite Images May Show Reprocessing Activity At North Korea Nuclear Site: U.S. Researchers*, REUTERS (Apr. 16, 2019), <https://reut.rs/2w52542>.

99. See Tariq Malik, *Scale of California’s Deadly Camp Fire Shown in Satellite Photos*, SPACE.COM (Nov. 11, 2018), <https://bit.ly/2H1AEyH>.

100. See Mark Bergen, *Startup Mapbox Makes Big Satellite Imagery Buy to Take On Google, Here Maps*, VOX (Oct. 28, 2015, 6:00 AM), <https://www.recode.net/2015/10/28/11620110/startup-mapbox-makes-big-satellite-imagery-buy-to-take-on-google-here>.

Earth.¹⁰¹ Of note for our Strava case study below, Mapbox is the company that created the final product used for the underlying imagery in the Strava heatmaps.¹⁰² Google Earth relies on multiple sources of images to function including satellite, aerial, 3D, and Street View images. Much of the imagery in Google Earth is created by stitching together a mosaic of multiple satellite and aerial images taken over a span of time. Using a mosaic allows Google Earth to present imagery that may have been obscured by clouds during the first collection.¹⁰³

GeoEye, now owned by DigitalGlobe, provides a further example of how the private sector is using data generated by remote-sensing satellite systems. GeoEye has a fleet of observation satellites that provide visible and near infrared (NIR) images of land and sea at resolutions below one meter.¹⁰⁴ GeoEye has provided 253 million square kilometers of satellite map images to Microsoft and Yahoo! search engines, and in 2013, Google obtained exclusive online mapping access to GeoEye's new GeoEye-1 satellite.¹⁰⁵ In addition, GeoEye was a major supplier of satellite generated data to the U.S. government's National Geospatial-Intelligence Agency.¹⁰⁶ With the purchase of GeoEye's companies and satellites, DigitalGlobe now fills that role.

Finally, Raytheon's recent entry into the commercial remote sensing field is worthy of a few observations. Raytheon, a defense contractor, developed and sells its SeeMe systems for defense and national security applications. SeeMe is part of a new wave of remote sensing satellites with the capacity to provide real-time imagery. On Raytheon's website, SeeMe is touted as a satellite provided to the Pentagon's Defense Advanced Research Projects Agency under the "Space Enabled Effects for Military Engagements," or SeeMe program. Raytheon explains, "the new small satellite will allow soldiers on the ground to see real-time pictures of the battlefield, which current military or commercial satellites cannot provide."¹⁰⁷ But the public summary of Raytheon's application and the commercial license issued by Commercial Remote Sensing Regulatory Affairs Office of the National Oceanic and Atmospheric Administration

101. See *How Images Are Collected*, GOOGLE EARTH, <https://support.google.com/earth/answer/6327779> (last visited June 20, 2019).

102. Nicki Dlugash, *Strava Maps for Runners and Cyclists*, MAPBOX: POINTS OF INTEREST (Nov. 3, 2015), <https://blog.mapbox.com/strava-maps-for-runners-and-cyclists-dbdb12a279c3>.

103. See *How Images Are Collected*, *supra* note 101.

104. *Id.*

105. *Id.*

106. *Id.*

107. *Id.*

(NOAA),¹⁰⁸ an agency of the U.S. Department of Commerce, presents another side to Raytheon's intended use and commercialization of its SeeMe system.¹⁰⁹

In 2015, Raytheon applied for and received a license from NOAA's Commercial Remote Sensing Regulatory Affairs Office to launch its SeeMe satellite, a private, commercial, space-based, remote sensing system.¹¹⁰ The SeeMe Satellite Remote Sensing License Public Summary, available on the NOAA website, describes the SeeMe as "the first" of the multiple satellites Raytheon is developing that is "capable of quickly providing . . . customers with imagery of their surroundings in real-time."¹¹¹ Raytheon's SeeMe satellite is "about the size of a water cooler and is cheaper to make and launch than the typical hardware sent into orbit."¹¹² SeeMe is equipped with "a camera and a telescope," with a rapid orbital period of "about 90 minutes."¹¹³ Raytheon envisions a constellation of SeeMe satellites, and one of the company's vice presidents explained, "[w]ith our automated production lines, Raytheon can produce large numbers of these highly reliable small satellites quickly and affordably."¹¹⁴

SeeMe's small size, mass-scale production potential, affordability, and rapid orbital path reflect the rapid technical advancements occurring in the commercial remote sensing industry. When combined with data from GPS tracking and smart devices, these advancements result in the aggregation of data in real-time with consequences that are hard to anticipate or control. To understand how these consequences come about, it is helpful to understand GPS satellite technology basics.

IV. SMART DEVICES

Smart devices, wearables, apps, social media platforms (like Strava), and wireless communications operate off the backbone of satellite data, and the private sector harnesses an array of satellite data in ways that are not appreciated by the public.

108. NOAA's role in regulation, licensing, and compliance enforcement of commercial remote sensing activities is discussed below in Section VI.C.

109. *See infra* Section VI.C.

110. *Raytheon Company: SeeMe Satellite Remote Sensing License Public Summary*, NAT'L OCEANIC & ATMOSPHERIC ADMIN. (Nov. 15, 2015), https://www.nesdis.noaa.gov/CRSRA/files/raytheon_company_noaa_license_public_summary.pdf.

111. *Id.*

112. *Id.*

113. *Id.*

114. *Small Satellite Work Ramps Up: Diminutive Devices Will Give Troops Real-time Battlefield Pictures*, RAYTHEON, https://www.raytheon.com/news/feature/small_satellites (last updated Mar. 05, 2019).

A. *Smart Devices and GPS Receivers*

As discussed in Section II.B., *supra*, GPS receivers are “chips” that can read the signals that GPS satellites broadcast. These receiver chips essentially read the digital radio signals at the frequency in which the satellites broadcast the digital signals, and also gather relevant time and location data from the digital signals.

Encouraged by affordability and Federal Communications Commission (FCC) mandates regarding location requirements for emergency services, most phones today have GPS receiver chips. The chips are small, inexpensive to manufacture, and consume little power.¹¹⁵ Because the FCC’s Enhanced-911 regulation mandates that cell network providers be able to provide relatively precise locations of persons placing 911 calls from mobile devices, the FCC E-911 regulation incentivized companies to include GPS receivers in mobile devices.¹¹⁶ Using GPS satellites, the receiver chips can pinpoint the user’s location without access to Wi-Fi or cellular service. For instance, if Corey was using a location service app like maps without internet access, Corey would still see a blue dot reflecting Corey’s location vis GPS, but the blue dot would appear to Corey on a blank map screen because Corey’s iPhone’s map app would be unable to download maps to view Corey’s position on the map application.

Wearable devices have built-in GPS receivers along with multiple types of sensors like motion sensors, optical sensors, etc. These wearable devices collect relevant data and once they are in contact with a phone via Bluetooth or the internet, these wearable devices send the data to the application servers, which store the data for processing and aggregation.

B. *Sensor-based Information Systems*¹¹⁷

The recent proliferation of cellular telephones and interconnected wearable devices provides a big solution to the limitations in GPS technology, albeit in a small size. In the 1980s, researchers developed

115. *Nano Chips Opens New Paths to Smaller Wearable Tech*, WEARABLE TECH. DIG., <https://www.wearabletechdigest.com/nano-chip-opens-new-paths-to-smaller-wearable-tech.html>.

116. *Enhanced 911 – Wireless Services*, FED. COMM’NS COMM’N, <https://www.fcc.gov/general/enhanced-9-1-1-wireless-services> (last visited June 20, 2019).

117. The authors gratefully acknowledge the invaluable research and writing assistance in this MEMS sensors section of Wyatt C. Weisenberg, Penn State Dickinson Law, J.D. anticipated May 2020.

microelectromechanical systems (MEMS) sensors.¹¹⁸ Breaking the word microelectromechanical apart provides an easy way to describe MEMS sensors:

micro- the size of the sensor is on the micrometer scale (one-millionth of a meter).

electro- the electric component powers the sensor and records the data.

mechanical- refers to mechanical functionality, i.e., a component that can stretch, deflect, spin, rotate, or vibration.¹¹⁹

Whereas GPS chips rely on signals from GPS satellites to geolocate, MEMS rely on tiny sensors that automatically translate tactile physical phenomena into digital information.¹²⁰

MEMS sensors are highly sensitive and provide a method of data collection with both an accurate spatial resolution and, importantly, a wide dynamic range.¹²¹ This dynamic range allows the utilization of MEMS with multiple sensors, each collecting different kinds of data.¹²² This dynamic range also allows MEMS with multiple versions of the same sensors, further increasing the amount and accuracy of data collection.¹²³ Since the 1980s, both manufacturing costs and the physical size of the MEMS have continually decreased, allowing the incorporation of MEMS into consumer-products at mass-scale.¹²⁴

MEMS sensors are primarily created using silicon,¹²⁵ which provides the MEMS' *sensing* abilities.¹²⁶ Silicon, itself, has many useful properties that allow for the inexpensive creation of MEMS sensors in a highly-pure

118. See Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 98 (2014) [hereinafter Peppet, *Regulating the IoT*]. "A MEMS device has electrical and mechanical components, which means there must be at least one moving or deformable part and that electricity must be part of its operation." JACOB FRADEN, *HANDBOOK OF MODERN SENSORS* 626 (4th ed. 2010) (ebook).

119. See FRADEN, *supra* note 118, at 364–65, 626–27 (describing MEMS sensors).

120. See Peppet, *Regulating the IoT*, *supra* note 118, at 99.

121. See FRADEN, *supra* note 118, at 364.

122. See Peppet, *Regulating the IoT*, *supra* note 118, at 99; FRADEN, *supra* note 118, at 364.

123. See FRADEN, *supra* note 118, at 364.

124. Alexander Wolf, *Little MEMS Sensors Make Big Data Sing*, FORBES (June 10, 2013), <https://www.forbes.com/sites/oracle/2013/06/10/little-mems-sensors-make-big-data-sing/>.

125. Note that silicon is a naturally occurring element, not to be confused with silicone, which is a synthetic compound that is unrelated to this paper.

126. See FRADEN, *supra* note 118, at 607–08 (describing the use of silicon in MEMS sensor).

laboratory setting.¹²⁷ MEMS sensors take advantage of silicon's inert physical effects including radiant,¹²⁸ mechanical,¹²⁹ thermal,¹³⁰ magnetic,¹³¹ and chemical.¹³² Manufacturers utilize silicon's inert characteristics because silicon does not require drastic alterations in order to create a sensor that measures these phenomena.¹³³ The nature of silicon provides half of the work for the manufacturer.

In addition to silicon's inert physical effects, MEMS sensors also take advantage of silicon's distinct physical characteristics during the manufacturing processes.¹³⁴ MEMS sensors rely on a series of microscopic and highly-precise mechanical structures.¹³⁵ Recall that the *mechanical* root in the term microelectromechanical refers to mechanical functionality.¹³⁶ For a visual reference of the scale and nature of MEMS sensors' microscopic and mechanical structures, imagine MEMS sensors not as a computer chip. Instead, imagine a wind farm filled with hundreds of individual wind turbines each responding to changes in the velocity of airspeed. Now take that windfarm and shrink it until it fits on the tip of a strand of hair. This is a MEMS system.

Manufacturers can create these structures using the same thin-film and photolithographic manufacturing techniques used when creating electronic circuits.¹³⁷ Naturally, manufacturers that can outfit their consumer devices with cutting-edge sensor technology that is highly precise, inexpensive, and uses the same manufacturing technique that

127. *See id.* The importance of a highly pure and inexpensive manufacturing environment cannot be overstated. Accuracy is a core characteristic of any technology that relies on sensors.

128. *Id.* Radiant physical effects of silicon include photoconductivity, photovoltaic, photoelectric, and photomagnetolectric effects, i.e., measurements of light and light wave properties.

129. *Id.* Mechanical physical effects of silicon include piezoresistivity, lateral photoelectric and lateral photovoltaic effects, i.e., measurements of force, pressure, vacuum, flow, tilt, thickness.

130. *Id.* Thermal physical effects of silicon include the Seebeck Effect, temperature dependence of conductivity and junction, i.e., measurements of temperature, temperature gradient, heat, entropy. The Seebeck Effect is a phenomenon in which heat is directly converted into electricity.

131. *Id.* Magnetic physical effects of silicon include magnetoresistance and the Hall and Suhi effects, i.e., measurements of magnetic field intensity, flux density, permeability.

132. *Id.* Chemical physical effects of silicon include ion-sensitivity field effects, i.e., measurements of concentration, toxicity, pH (acidity) levels, and reduction potentials.

133. *See* FRADEN, *supra* note 118, at 364 (describing MEMS sensors).

134. *See* FRADEN, *supra* note 118, at 364–65 (describing the use of silicon in MEMS sensor).

135. *Id.* (describing MEMS sensors).

136. *Id.*

137. *See* FRADEN, *supra* note 118, at 608.

company employs when producing electric circuits, will always choose to do so. Thus, we see the rise of phones, wearables, and everyday objects equipped with MEMS—the rise of the Internet of Things.¹³⁸ In 1999, researchers coined the term “Internet of Things” (IoT) to describe this process.¹³⁹ MEMS sensors are now present in cars, phones, health devices, and toys.¹⁴⁰

Cellular telephone and wearable device manufacturers are two industries that equip MEMS sensors into their products.¹⁴¹ Although the manufacturer advertises the phone’s many features, consumers are generally unaware that MEMS sensors are behind many of these new features.¹⁴² Subsequently, consumers are uninformed of how MEMS sensors interact with satellite-based technology.

Recall Corey’s journey home. Corey is using a navigation application that relies on the smart phones GPS chip to read the signals from GPS satellites that detail Corey’s location relative to the location of Corey’s house.¹⁴³ The navigation application also relies on MEMS sensors in the phone to assist in Corey’s journey. A magnetometer sensor on the phone acts as a compass by measuring the direction to the Earth’s ambient magnetic field.¹⁴⁴

On Corey’s drive home, Corey accidentally turns too sharply, causing the new phone to slide off Corey’s lap. Accelerometers, measuring the phone’s amount of acceleration, vibration, and tilt, record the speed Corey is driving and the speed of the phone as it slides off Corey’s lap.¹⁴⁵ When Corey retrieves the phone from the floor of the car, Corey accidentally holds it upside down. A gyroscopic sensor, recording the axis of the phone’s position, processes this data and automatically re-orientes the content on the screen from vertical to horizontal.¹⁴⁶

138. See Scott R. Peppet, *Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts*, 59 UCLA L. REV. 676, 699 (2012).

139. Duncan McFarlane, *The Origins of the Internet of Things*, REDBITE (Jun. 26, 2015), <https://bit.ly/2rFx5VY> (attributing the coining of the phrase, “Internet of Things,” to Kevin Ashton, co-founder of the Auto-ID Center at the Massachusetts Institute of Technology).

140. See Peppet, *Regulating the IoT*, *supra* note 118, at 98.

141. See Kevin Webach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2323 (2007) (describing the pervasiveness of networked sensors).

142. See Peppet, *Regulating the IoT*, *supra* note 118, at 145.

143. See *supra* notes 67-70 and accompanying text.

144. See *id.* The presence of a magnetometer sensor also allows phones to become a pseudo-metal detector. See Alexandr Balyberdin, *Metal Detector*, iTUNES STORE, <https://itunes.apple.com/us/app/metal-detector/id409682366?mt=8> (last visited June 20, 2019).

145. See Priyadarshini, *supra* note 67.

146. See *id.*

Cell phones are not the only devices equipped with MEM sensors. An ever-increasing array of smart devices contain many of the same sensors as phones and subsequently record much of the same data.¹⁴⁷ After successfully retrieving the phone from the car floor, Corey realizes that he is about to crash into another car. Corey's Fitbit, a wearable fitness tracker, records Corey's increased heart rate as he realizes the impending car crash.¹⁴⁸ The Fitbit lets Corey know that Corey's heart rate is above the average beats per minute and, as Corey's car is screeching to a stop, recommends a guided breathing session to aid in lowering Corey's heart rate.¹⁴⁹

The above hypothetical paints an admittedly incomplete picture of the scale of data creation, collection, and analytics following the mass integration of MEMS sensors into everyday life. Indeed, MEMS sensors surrounded Corey throughout the day, continuously collecting Corey's data. Corey's wearable device (with which Corey uses the Strava app) is embedded with MEMS sensors and a GPS chip. Corey's car has a host of MEMS sensors and a GPS chip—continually connecting with U.S. GPS satellites. Corey's home is replete with smart devices embedded with an array of MEMS sensors, GPS chips, and audio-video recording devices all collecting Corey and others' data, including Corey's doorbell, Corey's vacuum, Corey's personal assistant device, Alexa, Corey's smart TV, Corey's laptop, Corey's printer, Corey's iPad, and Corey's refrigerator. Corey's employment place provides no relief from this as Corey is also surrounded by MEMS sensor/GPS chip embedded smart devices.

Researchers estimate that by 2020, approximately 50 billion internet capable devices will have internet connectivity.¹⁵⁰ Worldwide shipments of MEMS is expected to grow to 20.2 billion individual units by 2022.¹⁵¹

147. Other common sensors include barometers (measures air pressure), proximity sensors (measures the distance between an object and the sensor), ambient light sensors (allows the device to adjust brightness), oscillators (for the internal clock). See David Nield, *All the Sensors in Your Smartphone, and How They Work*, GIZMODO (July 23, 2017), <https://gizmodo.com/all-the-sensors-in-your-smartphone-and-how-they-work-1797121002>.

148. See generally FITBIT, <https://www.fitbit.com/home> (last visited June 20, 2019).

149. See *Here's Why You'll Love Relax, Fitbit's New Guided Breathing Experience*, FITBIT (Aug. 29, 2016), <https://blog.fitbit.com/heres-why-youll-love-fitbits-new-guided-breathing-experience/>.

150. See Mariano-Florentino Cuellar, *A Simpler World: On Pruning Risks and Harvesting Fruits in an Orchard of Whispering Algorithms*, 51 U.C. DAVIS L.R. 27, 27 (2007).

151. David Manners, *MEMS to Take 73% of Sensor Market This Year*, ELECTRONICS WEEKLY (Sept. 5, 2018), <https://www.electronicsworld.com/news/business/mems-take-73-sensor-market-year-2018-09/>.

The growth of MEMS sensors alters society's acceptance of the incorporation of MEMS sensors into consumer devices and the amount of information that is collected. However, MEMS sensors and GPS chips in phones and other devices are merely *sources* of data.

C. *Software Applications*

Smart devices rely on programs and applications to interpret the data and allow users to interact with the data.¹⁵² While smart devices use proprietary programs created by the manufacturer to operate their various features, many devices also allow consumers to download applications and programs through a marketplace.¹⁵³ Recall that GPS receivers can calculate the location periodically and send it to the apps that have location access.¹⁵⁴ These apps then use this information to do whatever they need the location data to accomplish, *e.g.*, the Strava app.¹⁵⁵

Software developers, like Strava, create programs that use the GPS chips and MEMS sensors in the phone.¹⁵⁶ The openness of application marketplaces, as well as the desire to create the next *big* application, creates an extremely competitive application marketplace, where consumer preference trends towards free applications.¹⁵⁷ With traditional sources of revenue lost, application developers increasingly rely on data as a source of revenue.¹⁵⁸

How the phone and device applications interact with these sources of data is governed by agreements between the application marketplace, usually owned by the device manufacturer, and the developers.¹⁵⁹ A consumer that downloads the application can further limit the application's access to these sources of information.¹⁶⁰ The consumer's ability to limit application access to such information, however, is

152. See *supra* notes 67-70 and accompanying text.

153. See Artyom Dogtiev, *App Download and Usage Statistics (2018)*, BUSINESS OF APPS (updated Feb. 16, 2019), <http://www.businessofapps.com/data/app-statistics/> ("An app store (or app marketplace) is a type of digital distribution platform for smartphone, tablet, and software developers.").

154. See *supra* notes 67-70 and accompanying text.

155. See Robb, *supra* note 2 (describing the creation of Strava's Global Heatmap).

156. See *id.* (describing how Strava created their Global Heatmap through movement data provided by their users).

157. See Dogtiev, *supra* note 153 (noting the different types of marketplaces and the governance structure).

158. See generally Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1996).

159. See Dogtiev, *supra* note 153.

160. See *Advertising & Privacy*, APPLE (Sept. 17, 2018), <https://support.apple.com/en-us/HT205223> (describing application and advertising preferences).

hampered by application settings that require the consumer to affirmatively act to opt-out—consent is assumed by default.¹⁶¹

V. CASE STUDY: PRIVATE SECTOR AGGREGATION OF COMMERCIAL REMOTE SENSING, GPS, AND SENSOR DATA - THE STRAVA HEATMAP

Strava describes itself as “the social network for athletes.”¹⁶² The Strava app “syncs with most devices,” including “phone, GPS watch or head unit, heart rate monitor or power meter” to record user data and performance metrics.¹⁶³ Strava encourages users to share and upload to its platform user pictures and other data about user activities.¹⁶⁴ Strava provides a feature it calls “Beacon” that, when turned to “on” mode, enables Strava users to share their location in real time.¹⁶⁵ Beacon and other features of the Strava app are heavily dependent on GPS receiver and MEMS sensor data collected from synced user devices; this includes its trademark heatmap feature.¹⁶⁶ The scale of and amount of data depicted in the Strava heatmap is impressive: Strava’s heatmap reflects 700 million user activities, visualizes 1.4 trillion latitude/longitude points (gathered from user synced devices that collect GPS data), and 7.7 trillion pixels are rasterized to visually depict over 10 billion miles of user activities.¹⁶⁷ Remarkably, according to Strava, its “full global heatmap was built across several hundred machines in just a few hours, with a total compute cost of only a few hundred dollars.”¹⁶⁸

In creating its heatmap, Strava compiles data location tracks only from users who have consented to their geolocation data being collected. However, the default setting appears to be opt-in, and it is unclear if the functionality of certain app features is comprised when a user chooses to

161. *See id.*

162. *Features*, STRAVA, <https://www.strava.com/features> (last visited June 20, 2019).

163. *Id.*

164. *Id.* Uploaded pictures would necessarily include all metadata associated with the uploaded digital image file.

165. *Id.*

166. *Id.* However, it is unclear from Strava’s public information about its heatmap construction how much of this data is pure GPS location data or gathered from assisted-GPS (also using Wi-Fi and cellular location data). As discussed in Part IV, *supra*, most wearable devices and health apps use GPS to determine location at shortly-spaced periodic intervals and then upload the data onto the company servers. These devices have internal computational capacity to determine speed, elevation, etc. of the users. Further, most of the sensing components are independent of the internet, like motion sensors, accelerometers, temperature sensors, optical sensor to measure pulse, heartbeat sensors, etc.

167. *Id.*

168. *Id.*

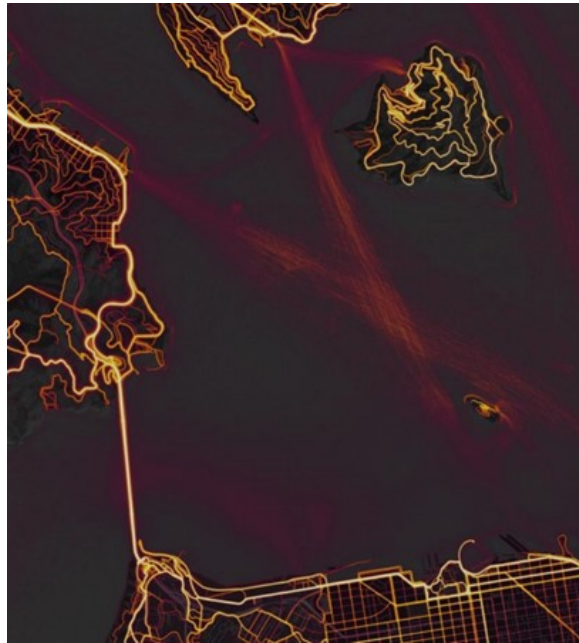
opt-out of location tracking and sharing. The heatmap depicts a snapshot of data aggregated from over a period of two years; and while Strava offers real time location tracking via the Beacon feature, the heatmap does not reflect activities in real time but only historical data. After the Strava heatmap reveal in January 2018, Strava now updates the heatmap every month to clear the data of the people who chose to not share their location.¹⁶⁹ The amount of information accumulated to generate the heatmap is about 5 Terabytes; for contextual reference, that is about as much data as the Hubble Space Telescope generates in 6 months!¹⁷⁰

Strava accumulates the raw activity data (running, biking, skiing, swimming) generated by the participating athletes, then goes through a series of steps to “clean up” the data, removing obvious errors.¹⁷¹ Incompatible corrections for location from other devices (such as GPS in smartphones) are addressed to create a quality-controlled activity dataset. These data are now accumulated by location into pixels with resolution of 4 square meters (about 43 square feet). This means that a runner covering 2 meters in a straight line will have moved from one pixel to another. These data are smoothed by a process known as rastering to create paths that capture how frequently that path has been used (the path “counts”). This is the raw heatmap data. Because we want to see all popular running paths, not just those along a bicycle path in the city or a university running track, Strava “normalizes” the paths. This means that the largest count value in an area about 5 km across is used to scale all of the other counts. For example, if 300 people run along the city bicycle path, 150 people use the university running track, and 75 people run along a local road, this will show up as 1 (hot), 0.5 (moderate) and 0.25 (cool) on the heatmap. Outside of the city, there may be only 20 runners along the river, and 5 runners along a trail; these values would show up as 1 (hot) and 0.25 (cool) on the heatmap for that rural location. In this way, athletes of all types and locations can see the popular locations for their sport.

169. *Heatmap updates*, STRAVA (Mar. 13, 2018), <https://blog.strava.com/press/heatmap-updates/>.

170. *Terabytes, Gigabytes, & Petabytes: How Big Are They?*, LIFEWIRE (Jan. 7, 2019), <https://www.lifewire.com/terabytes-gigabytes-amp-petabytes-how-big-are-they-4125169>.

171. See Robb, *supra* note 2. Examples of data that are excluded as errors are: athletes who have stopped moving but are still recording their location (which would otherwise create a bullseye on a heatmap), runners recording speeds typical of bicyclists, and runners or bicyclists recording speeds typical of cars or even airplanes.



In this figure of the San Francisco Bay area, Strava activity data has been normalized so that a wide range of heat data is visible in the image and values have been smoothed to change slowly across the region so that there are no sharp boundaries.¹⁷² The final activity data is combined with the Mapbox land image product (images that originated with DigitalGlobe) to

create a highly effective data visualization.

For purposes of this article and to grasp the complexity of the satellite and smart device data aggregation dilemma, it helps to remember two aspects of the Strava case study: (1) Strava collects copious amounts of user data, in some instances from multiple user-synced smart devices, including GPS, assisted-GPS location data using cellular data, along with other smart device MEMS sensor data to record intimate health details to measure user “performance” and (2) that the copious amounts of data, including GPS satellite data, being aggregated by Strava to create the heatmap are able to be processed for only a “few hundred dollars” of computing costs.¹⁷³

When Nathan Ruser tweeted about Strava’s recently published heatmap, the complex privacy and challenging national security implications resulting from inexpensive aggregation of smart device and readily available satellite data were on display for the world to see. As reported by *The Guardian*, in remote locations in Afghanistan, Djibouti and Syria, Strava users seem to be “almost exclusively foreign military

172. See Robb, *supra* note 2.

173. *Id.*

personnel.”¹⁷⁴ The end result: covert and forward operating bases stand out brightly on Strava’s heatmap.¹⁷⁵

VI. SATELLITES AND REMOTE SENSING: LEGAL AND REGULATORY FRAMEWORK

The scheme of international laws, treaties, domestic nation states’ laws, and organizational bodies that regulate and control satellite licensing, ownership, technical requirements, restrictions, and assignment of liability is byzantine. In this section, we note key international legal authorities governing satellites, address regulation of the U.S. GPS system, and then explain the U.S. regulatory and licensing regime for commercial remote sensing entities. Aspects of U.S. law that specifically regulate satellites from a national security perspective are discussed in Section VIII below, because national security-related satellite directives are integral to that section’s analysis of the national security implications created by satellite proliferation and satellite and smart device data aggregation by the private sector.

A. *International Law and Regulation*

The international legal regime governing satellite operations and communications is complicated and suffers from a siloed approach. First, it includes a body of law governing the use of outer space by governments and private actors, the most notable of which are: 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space (Outer Space Treaty); 1972 Convention on International Liability for Damage Caused by Space Objects (Liability Convention); 1975 Convention on Registration of Objects launched into Outer Space (Registration Convention); and 1987 Principles Relating to Remote Sensing of the Earth from Outer Space (UN Remote Sensing Principles). Second, the international framework governing satellites includes a body of law specific to communications and trade law, and includes the International Telecommunications Union (ITU), and the 1947 General Agreement on Tariffs and Trade (GATT).

While a full discussion of these authorities is beyond the scope of this article (and available in other sources¹⁷⁶), a few key principles are worth

174. Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret Location of US Army Bases*, THE GUARDIAN (Jan. 28, 2018), <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>.

175. *Id.*

176. See generally Frans G. von der Dunk, *Legal Aspects of Satellite Communications—A Mini Handbook*, J. TELECOMM. & BROADCASTING L., Sept. 2015, at 1 (India), available at <http://bit.ly/2EcTlrS>; Michael R. Hoversten, *U.S. National Security*

discussing. First, the concept of space as a “global commons” or “common interest.” This concept is derived from Article I of the Outer Space Treaty, which provides that outer space “shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies.” Similarly, Article II provides that outer space should not be subject to “national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.” Taken together, these provisions undergird the “global commons” principle: the idea that “states cannot dictate the activities of others in space.”¹⁷⁷ Second, the concept of “open skies” is particularly relevant to remote sensing activities. Embodied in a non-binding resolution, the “open skies” concept permits states to freely sense and distribute data from outer space without the consent of the sensed state.

B. Regulation of U.S. GPS System

As noted in Section III.B., the U.S. GPS is a satellite-based navigation system owned and developed by the U. S. Government. Pursuant to 10 U.S. Code § 2281, *Global Positioning System*, the U.S. GPS is regulated and operated by the U.S. Department of Defense (DOD). Section 2281(a) of the Code requires the Secretary of Defense to sustain “the capabilities” of GPS and the “operation of basic GPS services”¹⁷⁸ for the national security interests, and Section 2281(b) specifically directs the DOD to sustain and operate the GPS system for “civilian purposes.”¹⁷⁹

Civilian purposes are described as “peaceful civil, commercial, and scientific uses,” and DOD is directed to provide access to the GPS system “on a continuous worldwide basis free of direct user fees.”¹⁸⁰ Under the civilian purposes section, the Secretary of Defense is mandated to: coordinate with the Secretary of Transportation to develop and augment basic GPS to enhance civilian uses of GPS to support of transportation;¹⁸¹ coordinate with the Secretary of Commerce, the U.S. Trade

and Government Regulation of Commercial Remote Sensing from Outer Space, 50 A.F. L. REV. 253, 260–65 (2001).

177. Hoversten, *supra* note 176, at 261.

178. 10 U.S.C. § 2281 (2012 & Supp. 2017) defines “basic GPS services” as: “the following components of the Global Positioning System that are operated and maintained by the Department of Defense: (A) The constellation of satellites. (B) The navigation payloads that produce the Global Positioning System signals. (C) The ground stations, data links, and associated command and control facilities.”

179. *Id.* § 2281(b).

180. *Id.*

181. *Id.* § 2281(b)(2).

Representative, and other officials to facilitate development of “new and expanded civil and commercial” GPS uses;¹⁸² and to develop measures to prevent “hostile use of the GPS in a particular area without hindering peaceful civil use of the system elsewhere.”¹⁸³

It is a tall order: provide free, worldwide GPS satellite access and promote new and expanded civil and commercial uses of the system, but do not impair national security. The proliferation of GPS-enabled devices and the seamless integration of GPS data into app and IOT device functioning demonstrates DOD’s successful operation of the U.S. GPS system for civilian purposes. Smart devices embedded with GPS receiver chips, which use the U.S. GPS system as a means of geolocation, necessarily have used U.S. GPS compliant receiver chips. But the domination of the U.S. GPS system is under direct threat as China and other nations are developing and launching their own GNSS global satellite systems.¹⁸⁴ While many smart devices are currently manufactured embedded with GPS receiver chips compliant and compatible with the U.S. GPS system, that is rapidly changing as other nations are achieving full coverage with their own GNSS satellites.¹⁸⁵

C. *U.S. Regulation of Commercial Remote Sensing*

In the U.S., the federal agency that primarily regulates commercial remote sensing is the U.S. Department of Commerce’s National Oceanic and Atmospheric Administration (NOAA) and, to a lesser extent, the Federal Communications Commission (FCC).¹⁸⁶ For purposes of this article, we only focus on NOAA’s regulatory role and not FCC, because it is NOAA that operates the Commercial Remote Sensing Regulatory Affairs Office (CRSRA) and is tasked with licensing and regulating U.S. launched, commercially-owned remote sensing space systems.¹⁸⁷ It is curious and worthy of comment that NOAA, albeit an agency under the Department of Commerce, quietly regulates and licenses the U.S.’s multi-billion dollar commercial remote sensing industry. The average citizen more likely associates NOAA with weather and climate science.

182. *Id.* § 2281(b)(3).

183. *Id.* § 2281(b)(4).

184. *See supra* Section III.B.

185. *See supra* Sections III.B, IV.A.

186. Lewis & Caplan, *supra* note 85, at 10–11; *Compliance and Monitoring*, NAT’L OCEANIC & ATMOSPHERIC ADMIN., <https://www.nesdis.noaa.gov/CRSRA/complianceHome.html> (last visited June 20, 2019).

187. *See Compliance and Monitoring*, *supra* note 186.

NOAA's CRSRA currently operates under authority from the National and Commercial Space Programs Act of 2010¹⁸⁸ (NCSPA), the Land Remote Sensing Policy Act of 1992,¹⁸⁹ and pursuant to two presidential directives: the National Space Policy of the United States of America¹⁹⁰ (referred to as "U.S. National Space Policy") and the U.S. Commercial Remote Sensing Policy.¹⁹¹ NOAA's CRSRA can and does require specific limitations on the operational performance of commercial satellites.¹⁹²

NOAA's Commercial Remote Sensing Regulations are set forth in 15 C.F.R. Part 960, entitled, *Licensing of Private Land Remote-Sensing Space Systems*¹⁹³ (C.F.R. 960). Of note, the U.S. Department of Commerce and NOAA are currently revising C.F.R. 960, advanced notice of rulemaking was published in the Federal Register on June 29, 2018, with a goal of a full re-write of commercial remote sensing licensing regulations by December 2019. The stated purpose of the complete re-write of C.F.R. 960 is to "facilitate the continued growth of this critical industry and update the regulatory regime to address significant technological developments, new business models, and increased foreign competition"¹⁹⁴ While this advanced notice of rule-making was published in the Federal Register, it was not widely disseminated beyond that. During the notice period from June to August 2018, only ten comments were received. In reviewing the Advisory Committee on Commercial Remote Sensing (ACCRES) notes, there was no discussion of privacy and electronic surveillance concerns, the Fourth Amendment, or across-device data aggregation implications like the Strava scenario.¹⁹⁵

188. National and Commercial Space Programs Act of 2010, Pub. L. No. 111-314, 124 Stat. 3328 (2010) (codified as amended at 51 U.S.C.).

189. Land Remote Sensing Policy Act of 1992, Pub. L. No. 102-555, 106 Stat. 4163 (1992) (codified as amended at 51 U.S.C. ch. 601).

190. EXEC. OFFICE OF THE PRESIDENT, NATIONAL SPACE POLICY OF THE UNITED STATES OF AMERICA (June 28, 2010), *available at* https://www.nesdis.noaa.gov/CRSRA/files/national_space_policy_6-28-10.pdf [hereinafter NATIONAL SPACE POLICY].

191. REMOTE SENSING POLICY, *supra* note 39; *see also Authorities*, NAT'L OCEANIC & ATMOSPHERIC ADMIN., <https://www.nesdis.noaa.gov/CRSRA/generalAuthorities.html> (last visited June 20, 2019).

192. *Id.*

193. 15 C.F.R. pt. 960 (2018).

194. Licensing Private Remote Sensing Space Systems, 83 Fed. Reg. 30592 (proposed June 29, 2018).

195. *See generally 24th Meeting of the ACCRES Committee*, NAT'L OCEANIC & ATMOSPHERIC ADMIN., ADVISORY COMM. ON COMMERCIAL REMOTE SENSING (Oct. 18, 2018), https://www.nesdis.noaa.gov/CRSRA/pdf/ACCRES_24_Meeting_Minutes_final.pdf.

We address privacy and national security considerations for these new regulations below in Sections VIII and IX.

NOAA's CRSRA compliance and monitoring mission is "to facilitate the United States commercial remote sensing industry and promote collection and widespread availability of Earth remote sensing data, while preserving essential U.S. national security interests" ¹⁹⁶ In its introduction, the U.S. National Space Policy affirmatively acknowledges the commercial value and societal changes facilitated by commercial satellites in space, characterizing their use as the "now ubiquitous and interconnected nature of space capabilities and the world's growing dependence on them" ¹⁹⁷

The 2003 U.S. Commercial Remote Sensing Policy, a Presidential Directive, also provides authority for NOAA's CRSRA to regulate and support: (1) the licensing and operation of U.S. commercial remote sensing space systems; and (2) the United States Government use of commercial remote sensing space capabilities. To support its goals, the U.S. Commercial Remote Sensing Policy creates a strong and supportive marriage between the U.S. Government and private, commercial remote sensing actors, specifically stating in the Fact Sheet accompanying the Policy that the U.S. Government will:

- Rely to the maximum practical extent on U.S. commercial remote sensing space capabilities for filling imagery and geospatial needs for military, intelligence, foreign policy, homeland security, and civil users;
- Focus United States Government remote sensing space systems on meeting needs that cannot be effectively, affordably, and reliably satisfied by commercial providers because of economic factors, civil mission needs, national security concerns, or foreign policy concerns;
- Develop a long-term, sustainable relationship between the United States Government and the U.S. commercial remote sensing space industry;
- Provide a timely and responsive regulatory environment for licensing the operations and exports of commercial remote sensing space systems; and
- Enable U.S. industry to compete successfully as a provider of remote sensing space capabilities for foreign governments

196. *About Commercial Remote Sensing Compliance & Monitoring*, NAT'L OCEANIC & ATMOSPHERIC ADMIN., <https://www.nesdis.noaa.gov/CRSRA/complianceHome.html> (last updated Oct. 11, 2018).

197. NATIONAL SPACE POLICY, *supra* note 190, at 1.

and foreign commercial users, while ensuring appropriate measures are implemented to protect national security and foreign policy.¹⁹⁸

The U.S. National Space Policy specifically and intentionally advances commercial remote sensing for domestic society benefits,¹⁹⁹ while simultaneously the NOAA licensing requirements and C.F.R. 960 mandate that commercial remote sensing companies share data gathered from commercial remote sensing activities with the U.S. government. In the licensing application process, C.F.R. 960 mandates commercial remote sensing licensees to provide detailed information, including data safeguard practices and data sharing compliance.²⁰⁰ The NOAA CRSRA regulations (C.F.R. 960) provide application filing instructions, and 15 C.F.R. Section 960's Appendix 1 denotes specific information that must be included in the license application. The "Ground Segment"²⁰¹ and "Other Information"²⁰² sections of Appendix 1 requires licensees to provide the U.S. Government with detailed system data collection, data processes, upload and download controls, and other detailed information.

U.S. domestic law provides a regulatory framework that strongly supports private commercial remote sensing actors and promotes a close

198. REMOTE SENSING POLICY, *supra* note 39, at 2.

199. The U.S. National Space Policy introduction states: "The utilization of space has created new markets; helped save lives by warning us of natural disasters, expediting search and rescue operations, and making recovery efforts faster and more effective; made agriculture and natural resource management more efficient and sustainable; expanded our frontiers; and provided global access to advanced medicine, weather forecasting, geospatial information, financial operations, broadband and other communications, and scores of other activities worldwide. Space systems allow people and governments around the world to see with clarity, communicate with certainty, navigate with accuracy, and operate with assurance. The legacy of success in space and its transformation also presents new challenges . . ." NATIONAL SPACE POLICY, *supra* note 190, at 1.

200. 15 C.F.R. § 960.4 (2018).

201. 15 C.F.R. pt. 960, app. 1 (2018). "Ground Systems" information must include: the "system data collection and processing capabilities proposed including but not limited to: Tasking procedures; scheduling plans; data format (downlinked and distributed data); timeliness of delivery; ground segment information regarding the location of proposed operations centers and stations, and tasking, telemetry and control; data distribution and archiving plans; the command (uplink and downlink) and mission data (downlink) transmission frequencies and system transmission (uplink and downlink) footprint, the downlink data rate, any plans for communications crosslinks." *Id.*

202. *Id.* The "Other Information" sections of Appendix 1 require licensees to provide NOAA with, "[t]he applicant's plans for providing access to or distributing the unenhanced data generated by the system including: A description of the plan for the sale and distribution of such data; The method for making the data available to governments whose territories have been sensed; A description of the plans for making data requested and purchased by the Department of the Interior available to the National Satellite Land Remote Sensing Data Archive for inclusion in the basic data set. . ." *Id.*

relationship between the U.S. government, U.S. national security interests, and the commercial sector in space. The policies of strongly supporting commercial remote sensing activity in space, while maintaining regulatory oversight over and requiring data sharing from the same commercial remote sensing actors, foster significant economic growth in the U.S. commercial remote sensing private sector. The policies enable the U.S. government to harness and share the benefits of the private sector's rapid technical achievements in satellite surveillance capabilities and have access to the wealth of data afforded from the same surveillance capabilities, while avoiding potential *posse comitatus* concerns.

Because commercial remote sensing activity occurs in the "open skies" of "space," the regulation of commercial remote sensing occurs wholly distinct from the U.S. domestic electronic surveillance scheme. The latter embodies and secures the constitutional right to privacy against unwarranted or overly intrusive surveillance by the U.S. government. In their current form, commercial remote sensing regulations fail to consider or even adhere to U.S. domestic electronic surveillance laws and constitutional privacy concerns. But we do so in the next section.

VII. SATELLITES AND SMART DEVICES: U.S. LAW AND PRIVACY CONCERNS

Above, we discussed the impending rewrite of C.F.R. 960, which regulates the commercial remote sensing licensing process. The new C.F.R. 960 regulations are intended to go into effect in December 2019, although at the time this article goes to the publisher, the text of the proposed regulations have not been made publicly available. During a presentation at the National Space Council meeting in Washington, D.C., on Oct. 23, 2018, Karen Dunn Kelley, then acting deputy secretary of commerce, announced that the department had just submitted to the Office of Management and Budget (OMB) the draft rule revising C.F.R. 960.²⁰³ Dunn Kelley stated the new C.F.R. 960 "will revolutionize the way we regulate the use of cameras in space." Her comments lauded the commercial benefits that would flow from the new rule's unfettering of regulatory restrictions on what commercial actors can do in space, saying it would "replace outdated regulation[s] that are slowing down industry achievements." The new rule, she said, would create categories that "exempt certain pre-approved activities" from a lengthy license application and review process . . . But Dunn Kelley's comments made no mention of privacy or domestic electronic surveillance, and she did not

203. Jeff Foust, *Revised Remote Sensing Regulatory Rule Nears Release*, SPACENEWS (Oct. 26, 2018), <https://spacenews.com/revised-remote-sensing-regulatory-rule-nears-release/>.

address in any way the subject of data aggregation from satellites and smart devices.²⁰⁴

While commercial remote sensing is heavily regulated by U.S. domestic law, because commercial remote sensing occurs in “space,” its regulation has little to no intersection with the long-developed U.S. scheme of domestic electronic surveillance and associated jurisprudence. But a review of 15 C.F.R. 960’s Appendix 1, the information required for licensing requirements, reveals just how much of the data processing and data use derived from commercial remote sensing takes place using “Ground Systems.” It is a curious disconnect because commercial remote sensing companies use satellites to engage in domestic electronic surveillance and do so through systems, processes, and algorithms obviously tethered to the planet.

This same hands-off approach to satellite-derived data can be seen in the collection or use of GPS-based geolocation data, which largely occurs in a regulatory void. The FCC and the FTC classify geolocation services as “sensitive information” and urge a heightened need for protection of privacy, but such protection is not actually mandated by federal statute.²⁰⁵ The FTC recommends “just-in-time” disclosures to consumers, which is disclosure at the time of collection, to obtain their affirmative consent, and it also recommends that apps provide consumers with a privacy dashboard and icons indicating that location information is being collected among others. If the app collects geolocation data over time, the disclosure should not give the impression that it is a one-time collection.

To fully appreciate the confounding nature of the disconnect in law between satellite surveillance and domestic electronic surveillance and privacy concepts, we will briefly overview U.S. privacy law concepts and the U.S. domestic electronic surveillance laws and jurisprudence.

204. *Id.*

205. FED. TRADE COMM’N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2010), <http://bit.ly/2M55cnN>; Alan Murray, *FTC Wants to Beef Up Mobile Privacy Disclosures*, WIRED (Mar. 4, 2013), <https://www.wired.com/insights/2013/03/ftc-wants-to-beef-up-mobile-privacy-disclosures/>.

A. *Constitutional Concepts of Privacy*²⁰⁶

The word “privacy” does not appear in the United States Constitution,²⁰⁷ but in their seminal 1890 Harvard Law Review article, *The Right to Privacy*, Samuel Warren and Louis Brandeis framed our modern constitutional and common law concepts of privacy.²⁰⁸ In large part due to Warren and Brandeis’ article, the U.S. Constitution—despite missing the magic *privacy* word—is the cornerstone of modern privacy law.²⁰⁹ Common law privacy concepts and the common law right to privacy have flowed therefrom and, as evidenced by the amount of civil litigation cases asserting invasion of privacy-based claims, the U.S. common law provides for a right to privacy.

There are some marked similarities between the issues presented by the satellites, smart devices, and IoT data aggregation and those that prompted Warren and Brandeis to write their article in 1890. These issues are three-fold: (1) legally unfettered gathering of personal data (2) by private industry for commercial gain (3) enabled through advanced technologies. In the satellite-smart device-IoT era, these factors combine to foster invasions of individual privacy on a scale heretofore unimaginable.

In the 1965 case, *Griswold v. Connecticut*,²¹⁰ the U.S. Supreme Court first recognized a constitutional right to privacy flowing from rights afforded to citizens in the First, Third, Fourth, Fifth, and Ninth Amendments to the U.S. Constitution.²¹¹ Many of the Court’s decisions involving the constitutional right to privacy and enhanced forms of government surveillance involve the Fourth Amendment,²¹² and its Fourth Amendment jurisprudence has a long and sometimes convoluted, but continually evolving, history. A full overview of this history is beyond the scope of this article. But to understand the disconnect that currently exists between commercial remote sensing data collection and remote sensing

206. For a more detailed discussion of the history and development of U.S. privacy law, see generally Anne T. McKenna, *Pass Parallel Privacy Standards or Privacy Perishes*, 66 RUTGERS L. REV. 1041 (2013).

207. See U.S. CONST.; see also Mark Silverstein, Note, *Privacy Rights in State Constitutions: Models for Illinois?*, 1989 U. ILL. L. REV. 215, 218 (1989).

208. See generally Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890).

209. See generally *id.*

210. *Griswold v. Connecticut*, 381 U.S. 479 (1965).

211. *Id.* at 483–85.

212. The Fourth Amendment to the United States Constitution provides: “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV.

data sharing with the government on the one hand, and U.S. Supreme Court jurisprudence and the U.S. domestic electronic surveillance scheme on the other, some background is necessary.²¹³

In the next sections, we address the Court's Fourth Amendment jurisprudence, and because commercial remote sensing entities are engaged in electronic surveillance and location tracking, and the fruits of that surveillance may be shared with the U.S. government by regulatory fiat, we also briefly summarize the U.S. domestic electronic surveillance statutory scheme.

B. The Fourth Amendment and a Disconnect in Aerial Surveillance/Location Tracking Jurisprudence

The Fourth Amendment prohibits unreasonable searches and seizures, but it applies only to government search and seizure.²¹⁴ It does not apply to private industry or third-party search and seizure.²¹⁵ For decades, the U.S. Supreme Court has considered the constitutionality of searches conducted with technology that enhances a human's own ability to see, follow, feel, hear, or smell. The cornerstone of modern Fourth Amendment jurisprudence and enhanced surveillance technology centers around the concept of a reasonable expectation of privacy. In the 1967 *Katz v. United States*²¹⁶ case, the Court held that it violated the Fourth Amendment to attach a listening device to a public telephone booth. Justice Harlan's concurrence set the stage for a major development in our modern-day concept of privacy, which is that one must have a reasonable expectation of privacy for society and the law to recognize it and protect it.

In the Court's evolving Fourth Amendment and constitutional privacy jurisprudence, willful or knowing disclosure of information took on greater significance. If you knowingly exposed something to the public or voluntarily turned information over to someone else (a third party), you could not claim to have a reasonable expectation of privacy. Voluntarily turning information over to another formed the basis of the Court's Third-Party Doctrine.²¹⁷

213. We note that satellite surveillance also poses significant First Amendment concerns, but that is for another article.

214. *See* *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).

215. *See id.* at 117.

216. *Katz v. United States*, 389 U.S. 347, 353 (1967).

217. *Smith v. Maryland*, 442 U.S. 735, 744 (1979). The defendant in *Smith* had disclosed the phone numbers he dialed out to the telephone provider. *Id.* at 745. The Court

In its framework of jurisprudence addressing enhanced forms of surveillance, the Court has ruled that the government's warrantless uses of wiretaps,²¹⁸ dog sniffing,²¹⁹ thermal imaging,²²⁰ attachment and use of a physical GPS device,²²¹ and obtaining historical cell site location information (CSLI) for tracking purposes²²² are all unlawful violations of the Fourth Amendment. But the warrantless use of aerial surveillance does not violate the Fourth Amendment.²²³

When it comes to applying this framework of rulings to satellite remote sensing data and its aggregation with smart device data, the disconnect in the Court's jurisprudence becomes apparent. On the one hand, warrantless enhanced aerial surveillance by law enforcement is lawful, while on the other hand, law enforcement's warrantless persistent location tracking by enhanced technologies is unlawful. Specifically, in its 2018 *Carpenter* decision, the Court ruled that warrantless location tracking via CSLI was unlawful.²²⁴ *Carpenter* was preceded in 2012 by the Court's *U.S. v. Jones* decision, wherein the Court ruled that the warrantless attachment and use of a GPS tracking device to a suspect's car was unlawful. Justice Sotomayor's concurrence frames privacy and civil liberties concerns that apply equally to satellite data as well:

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may “alter the relationship between citizen and government in a way that is inimical to democratic society.”²²⁵

held that this voluntary disclosure to the telephone provider was third party disclosure, and thus the data was no longer afforded Fourth Amendment protection. *Id.*

218. See *Katz*, 389 U.S. at 359 (1967).

219. *Florida v. Jardines*, 569 U.S. 1, 11 (2013).

220. *Kyllo v. United States*, 533 U.S. 27, 40 (2001).

221. *United States v. Jones*, 565 U.S. 400, 412–13 (2012).

222. *Carpenter v. United States* 138 S. Ct. 2206, 2223 (2018).

223. See *Dow Chemical Co. v. United States*, 476 U.S. 227, 239 (1986); see also *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (ruling that there was no Fourth Amendment violation when officers flew over a private residence at 1000 feet and took photographs after receiving a tip about a marijuana grow operation; *Florida v. Riley*, 488 U.S. 445, 452 (1989) (ruling that photographs taken from a helicopter at 400 feet over a private residence did not constitute a search); *FISHMAN & MCKENNA*, *supra* note 9, § 30:13.

224. See *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

225. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring) (citing *United States v. Cuevas-Perez*, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

The legal conclusions drawn from these two categories of enhanced surveillance cases (the aerial surveillance cases and the enhanced, persistent location tracking cases), while perhaps rational in the historical context in which each decision was reached, pose a head-on conflict. GPS satellites combined with smart devices embedded with GPS chips allow real-time location tracking. The reality is that commercial remote sensing actors, device manufacturers, and apps aggregate, use, disseminate, and sell satellite data, GPS chip data, and smart device data and, thus, engage in persistent location surveillance. Commercial remote sensing activities and capabilities are evolving so rapidly (consider Raytheon's SeeMe satellite) that real-time tracking through images alone is becoming reality. In the case of commercial remote sensing entities, U.S. government access to the data is permitted by the licensing regulations.

C. *The U.S. Electronic Surveillance Statutory and Data Scheme*

U.S. satellites are governed by space and communications law and NOAA's regulatory oversight, rather than domestic electronic surveillance laws, data laws, and constitutional concepts of privacy. We consider briefly in this section the U.S. domestic electronic surveillance scheme because the existing U.S. domestic electronic surveillance scheme embodies the Fourth Amendment and privacy protections developed through the Court's jurisprudence, which is discussed in the preceding section. In the U.S., electronic surveillance and data protections are regulated at both the federal and state levels. While some states, like California,²²⁶ Illinois,²²⁷ and Maryland,²²⁸ have enacted laws that afford greater data privacy protection and stronger protections from electronic

226. See California Online Privacy Protection Act, CAL. BUS. & PROF. CODE §§ 22575–79 (West 2019).

The California Online Privacy Protection Act (CalOPPA) applies to commercial website and mobile app operators that collect personally identifiable information (PII), which is broadly defined by the statute. CalOPPA requires website operators to conspicuously link to a Privacy Policy on their website that discloses what type of personal information is collected through the online service (website and/or mobile app) and with what third parties the collected PII may be shared. There is no overarching federal law that protects PII.

227. Illinois passed its Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. 14/1–14/99, in 2008. BIPA affords protection to biometric identifying information and requires notice and consent for collection of specifically defined biometric identifiers. See 740 ILL. COMP. STAT. 14/15 (West 2019). There is no federal biometric information privacy law.

228. Maryland's wiretapping statute, MD. CODE ANN., CTS. & JUD. PROC. § 10-402 (West 2019), requires all-party consent to recording of communications whereas federal law, only requires one party to consent to the recording of a communication. 18 U.S.C. § 2511(2)(c)–(d) (2012 & Supp. 2017).

surveillance than federal law, in this brief overview, we focus exclusively on the federal electronic surveillance statutory scheme.²²⁹ Because there currently is no overarching U.S. federal data privacy law, and there is no specific federal law governing personal data generated by the satellite-smart device information nexus, we have not overviewed the U.S. data law framework.²³⁰ As we note in our recommendation section, however, the privacy, civil liberty, and national security issues resulting from the satellite-smart device information nexus (and its data) demand legislative attention.

The Electronic Communications Privacy Act (ECPA)²³¹ regulates the interception of wire, oral, and electronic communications by government and private actors. Through Title III as amended by ECPA, Congress has sought to safeguard the privacy of wire, oral, and electronic communications and, in particular, the privacy of innocent persons.²³² ECPA forbids the interception of wire, oral or electronic communications by private persons unless the communication is intercepted by, or with the consent of, a participant, and significantly restricts the authority of law enforcement officials to intercept such communications.²³³

ECPA, passed in 1986, was an effort by Congress to bring advancing electronic communications platforms and technology, including cellular phones and location tracking, within the scope of Title III's protection and regulation afforded wire and oral communications.²³⁴ For instance, ECPA amended Title III's definition of wire communication by specifying that aural transmission constitute wire communication despite the use of radio waves and not wires, so long as a switching station creates the connection between the sending and receiving phones.²³⁵ As noted in the Senate Committee report: "[T]his . . . makes clear that cellular communications—whether they are between two cellular telephones or between a cellular telephone and a 'land line' telephone—are included in the definition of 'wire communications' and are covered by the statute."²³⁶

Two federal statutes directly address law enforcement's use of cellular devices as mobile tracking devices: 18 U.S.C. § 3117, entitled

229. For an in-depth analysis of electronic surveillance law in the U.S., we direct the reader to FISHMAN & MCKENNA, *supra* note 9.

230. That, too, is the subject of another article.

231. See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

232. See Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801(b), 82 Stat. 197, 211 (1968); S. REP. NO. 90-1097 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2177; *see also* State v. Gilmore, 549 N.W.2d 401, 405 (Wis. 1996) (citing FISHMAN & MCKENNA, *supra* note 9).

233. See 18 U.S.C. § 2511.

234. See FISHMAN & MCKENNA, *supra* note 9, at § 1:15.

235. See Electronic Communications Privacy Act, § 101(a)(6).

236. S.Rep. 99-541, 99th Cong. 2d Sess. reprinted in 1986 U.S.C.C.A.N. at 3565.

“Mobile tracking devices,”²³⁷ which regulates the use of tracking devices that move across state lines; and 47 U.S.C. § 1002, part of the Communications Assistance for Law Enforcement Act (CALEA),²³⁸ which we discuss briefly below. In the Mobile Tracking Devices statute, ECPA broadly defines “tracking device” to mean “an electronic or mechanical device which permits the tracking of the movement of a person or thing.”²³⁹

In application of these statutes to cell phones tracking, we also briefly mention ECPA’s Pen Register Trap and Trace Statute (the “Pen/Trap Statute”),²⁴⁰ which regulates the use of pen/trap devices, and the Stored Communications Act (SCA).²⁴¹ The Pen/Trap Statute governs real-time interception of “the numbers dialed or otherwise transmitted on the telephone line to which such device is attached.”²⁴² To date, a Rule 41 warrant based upon probable cause has been necessary to authorize and install a mobile tracking device.²⁴³ The Pen/Trap Statute only requires a certification that the pen/trap device may obtain information relevant to an ongoing investigation.²⁴⁴ It specifically provides that:

a government agency authorized to install and use a pen register or trap and trace device under this chapter . . . shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.²⁴⁵

237. See 18 U.S.C. § 3117 (2012 & Supp. 2017).

238. See Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 and 47 U.S.C.).

239. 18 U.S.C. § 3117(b).

240. 18 U.S.C. §§ 3121 to 3127.

241. 18 U.S.C. § 2703.

242. The Pen/Trap Statute, enacted as part of ECPA, governs real-time interception of “dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication.” Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 3126(3), 100 Stat. 1848, 1871 (1986) (amended 2001). The standard is that of a rubber stamp. See *CDT’s Analysis of S. 2092: Amending the Pen Register and Trap and Trace Statute in Response to Recent Internet Denial of Service Attacks and to Establish Meaningful Privacy Protections*, CTR. FOR DEMOCRACY & TECH. (Apr. 4, 2000), <https://www.cdt.org/files/security/000404amending.shtml>.

243. See *United States v. Jones*, 565 U.S. 400, 405 (2012).

244. 18 U.S.C. § 3122(b)(2) (2012 & Supp. 2017).

245. 18 U.S.C. § 3121(c) (2012 & Supp. 2017).

Information that communication service providers may produce to law enforcement pursuant to the Pen/Trap Statute is specifically limited by CALEA.²⁴⁶ CALEA forbids the provider from producing “*any information that may disclose the physical location of the subscriber*” when the provider is producing call identifying information pursuant to the Pen/Trap statute.²⁴⁷

ECPA’s Stored Communications Act (SCA), found at 18 U.S.C. §§ 2701 to 2712, authorizes government access to stored communications in the hands of third-party providers.²⁴⁸ The SCA categorizes different types of stored communications (information) and what the government must do to obtain access to those different types of information.²⁴⁹ The protection afforded by the SCA to these different types of information is based upon the type of stored information sought, i.e. is it addressing or dialing information (which is afforded the least protection), or is it “content” information (which is afforded the greatest protection from surveillance).²⁵⁰

This brief overview of certain elements of our complex federal electronic surveillance legislative scheme is to demonstrate that Congress intended, through these laws, to protect U.S. citizens’ electronic communications, cellular communications, and location information. However, this complex scheme typically does not apply to private industry’s tracking of and data aggregation from individuals via the satellite-smart device information nexus. We discuss that information nexus in more detail in our next section.

D. *Privacy and Civil Liberty Concerns*

Satellite-based information systems and sensor-based information systems have merged into an information nexus. The satellite-smart device information nexus is best understood as a chain of information collection technologies,²⁵¹ laws and regulations,²⁵² and agreements²⁵³ between multiple actors. As noted above, the U.S. government provides public access to GPS satellites. Phone manufacturers are in essence required to

246. See Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 and 47 U.S.C.).

247. 47 U.S.C. § 1002(a)(2)(B) (2012 & Supp. 2017) (emphasis added).

248. See 18 U.S.C. §§ 2701–12 (2012 & Supp. 2017).

249. See *id.*

250. See *id.*

251. See *supra* Parts III (describing satellite technology), IV (describing smart device technology).

252. See *supra* Parts VI (describing satellite laws and regulations), VII (describing smart device laws and regulations).

253. See, e.g., APPLE, *supra* note 160.

equip phones with a GPS receiver.²⁵⁴ Manufacturers increasingly equip devices with MEMS sensors. Devices increasingly use third-party applications. Third-party applications use GPS receivers and MEMS sensors both for the function and as a source of revenue.²⁵⁵

Unfortunately, these actors are often concerned with only one chain of the information nexus at a time. For example, application developers who create a GPS application view the nexus through that interaction and fail to consider the relationship between the GPS application and the device's MEMS sensors. Manufacturers who equip their MEMS sensors similarly view the nexus through that interaction and fail to consider the relationship between the sensors and the GPS receivers.²⁵⁶

The result: data aggregation from commercial remote sensing activities combined with smart devices and IoT realities have created a dramatically altered privacy landscape with significant national security and civil liberties impacts. While scholars agree that privacy norms continue to shift with technological advances and the proliferation of social media sites and other information sharing platforms,²⁵⁷ the public and legislators appear unaware of both the vast surveillance capabilities of commercial remote sensing activities and, when combined with data aggregated via smart device sensors, the current state of complete surveillance of all persons' locations, physical status, and their proximity and relationship to other persons at all times. The continued disconnect between the regulation of commercial remote sensing activities, the regulation of data aggregation from smart device sensors and IoT devices, and current U.S. electronic surveillance law and U.S. Supreme Court decisions leads to confusion, lack of citizen awareness, and enables situations like the Strava case study.

VIII. SATELLITE DATA AND SMART DEVICES: NATIONAL SECURITY CONCERNS

In the wake of the Strava heatmap incident, many wondered how the U.S. Department of Defense was so blindsided? How did it fail to see the

254. See 10 U.S.C. § 2281(b) (2012 & Supp. 2017).

255. Compare Robb, *supra* note 2 (using the smart device's GPS receiver), with Balyberdin, *supra* note 144 (using the smart device's MEMS sensors).

256. Compare Sarah Williams, *More than Data: Working With Big Data for Civics*, 11 I/S: J. L. & POL'Y 181, 192–93, 196 (2015) (failing to note the legal implications of data collection), with Cuellar, *supra* note 150, at 30 (discussing the impact of AI on markets, politics, institutions, and societal norms, as well as the need to structure laws in recognition of the growth and impact of AI).

257. Basil A. DiSipio, *Global Positioning Systems and Social Media—Anathemas to Privacy*, DEF. COUNSEL J., Oct. 2017, at 1, 1–5.

impact that the aggregation of satellite data would have on impact national security? In our view, there are two main reasons the U.S. government failed to recognize or appreciate the scope of the threat. First, the U.S. military was focused on different types of threats to satellites—threats from malicious actors, threats of physical destruction, and threats from cyber operations. The U.S. military did not anticipate or fully appreciate the impact that non-malicious aggregation of publicly-available satellite data could have on national security. Second, a cumbersome legal regime coupled with the U.S. policy promoting private sector ownership of remote sensing satellites impeded U.S. national defense entities from identifying the harmful impact of GPS and smart device data. This is not a new problem. The U.S. government has struggled for years to achieve the appropriate balance between national security concerns and commercial interests in exploring and using space. Although not new, the struggle is more urgent with the coming of 5G networks and increasing number of satellites with remote sensing capabilities.

This section describes and analyzes the specific threats posed by the aggregation of commercial satellite data to U.S. national security. It examines why the U.S. government was surprised by the Strava heatmap incident and failed to anticipate similar threats. It next considers the legal authorities that permit the U.S. government to restrict the collection, use, and dissemination of remote sensing data in the interest of national security, describes the current regime's shortcomings and previews developments in the law. Finally, it explains why the Strava incident was not a one-time concern, but reflective of a growing and persistent challenge.

The U.S. civilian economy is “heavily dependent” on satellites for a variety of functions.²⁵⁸ Satellite-provided services are so “ubiquitous” that we neither notice their origin,²⁵⁹ nor do we fully appreciate the breadth and depth of our reliance on the availability, integrity, and reliability of satellite-provided data and services.²⁶⁰ Indeed, at least one scholar has referred to satellites as the “Achilles heel” of the U.S. civilian economy, noting that any disruption to the availability, integrity, and reliability of satellites will have significant—and likely adverse—impacts.²⁶¹

258. See Francis Grimal & Jae Sundaram, *The Incremental Militarization of Outer Space: A Threshold Analysis*, 17 CHINESE INT'L L.J. 45, 54 (2018).

259. See David A. Koplow, *The Fault is Not in Our Stars: Avoiding An Arms Race in Outer Space*, 59 HARV. INT'L L.J. 331, 332 (2018).

260. *Id.* at 331–32. As Professor Koplow writes, “[We are] passively unaware of how thoroughly our daily activities, and our responses to military crises, have become reliant upon a secure, predictable regime of outer space” *Id.* at 332.

261. See *id.* at 331 – 37 (“[S]atellites may now be the Achilles heel of the American civilian economy and its mighty military apparatus.”); Michael Nayak, *CubeSat Proximity Operations: The Natural Evolution of Defensive Space Control into a Deterrence*

Like the U.S. civilian economy, the U.S. military is dependent on satellites. It depends on satellite-generated data for communications, surveillance, early warning systems, navigation, signals intelligence, and meteorology.²⁶² Given this dependence, how did the U.S. military not anticipate the threat presented by a company like Strava that was collecting, aggregating and sharing data from remote sensing satellites?

A. *The Strava Heatmap: Understanding the National Security Impacts from the Aggregation of Remote Sensing Data and Smart Devices*

To appreciate the scope of the data aggregation threat, it is helpful to be specific about the information the Strava heatmap revealed. On January 27, 2018, Nathan Ruser's tweet stated, "If soldiers use the app like normal people do, by turning it on tracking when they go to do exercise, it could be especially dangerous."²⁶³ It was "dangerous" for a number of reasons. However, from a national security perspective, the Strava heatmap created four distinct types of security risk.

First, the heatmap identified the boundaries of previously unknown or secret U.S. military bases around the world.²⁶⁴ To put it bluntly, as one headline did: "Fitness app Strava lights up staff at military bases."²⁶⁵ Second, the aggregation of users' GPS data into a global heatmap revealed patrol routes, as well as military supply and transportation routes and may have identified other previously unknown facilities as a user moved from a known military base to other military facilities.²⁶⁶ "[T]he bigger worry from an operations security standpoint [is] how Strava's activity data could be used to identify interesting individuals, and track them to other

Initiative, SPACE REV. (Jan. 18, 2016), <http://www.thespacereview.com/article/2902/1> ("Foreign policy analysts have not missed this Achilles heel either.").

262. See Grimal & Sundar, *supra* note 258, at 54.

263. Nathan Ruser (@Nrg8000), TWITTER (Jan. 27, 2018, 10:56 AM), <https://twitter.com/Nrg8000/status/957326421684207616>.

264. See *Fitness app Strava lights up staff at military bases*, BBC NEWS (Jan. 29, 2018), <https://www.bbc.com/news/technology-42853072> (appearing to show the structure of foreign military bases in countries including Syria and Afghanistan as soldiers move around them); see also Jeremy Hsu, *The Strava Heat Map and the End of Secrets*, WIRED (Jan. 29, 2018, 7:14 PM), <https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/>.

265. See BBC NEWS, *supra* note 264; see also Liz Sly et al., *U.S. military reviewing its rules after fitness trackers exposed sensitive data*, WASH. POST (Jan. 29, 2018), <https://wapo.st/2w5OWrz>.

266. See Hsu, *supra* note 264 ("You could for example identify somebody who works at a known secret facility and then track his movements to other facilities through which he may rotate.").

sensitive or secretive locations.”²⁶⁷ Third, depending on how a user set their privacy settings in the app, the interactive capability of the map revealed the identities and locations of specific individuals.²⁶⁸ “Once you can identify individuals the data becomes a lot more valuable,” said Tobias Schneider, a Berlin-based security analyst.²⁶⁹ One Strava user demonstrated how to use the heatmap and Google to identify by name a U.S. Army major and his running route at a base in Afghanistan.²⁷⁰

Fourth, and finally, this is not a problem specific to military personnel. The heatmap also revealed information about humanitarian and aid workers and their routes and operations.²⁷¹ In 2018, a former peacekeeper noted that he was able to use the map to pinpoint the jogging route he used when he served with U.N. peacekeepers in South Sudan.²⁷² He used similar sites to identify the names and daily routines of eight foreigners working for aid agencies and the United Nations in the Somali capital Mogadishu, noting that the “focus of this story has been soldiers and spies, but we are also talking about humanitarian workers. If you look at what we saw in Mogadishu and you are al-Shabab, you get a pretty good idea of who the foreigners are and where they are working.”²⁷³

To be clear, Strava violated no laws in creating the global heatmap or in making it publicly available. Likewise, the Strava users who failed to use the most rigorous privacy settings when setting up the app did nothing illegal, although many have since changed those settings. Rather, the consequences of aggregating publicly available GPS data, gathered from users of wearable connected devices, came as an unwelcome surprise to many. So how did the U.S. military, which is heavily dependent on and invested in the use of remote sensing satellite data, fail to appreciate this surprise?

267. *Id.* (noting that researcher and activist Paul Dietrich claimed to use public data scraped from Strava’s website to track a French soldier from overseas deployment back to France).

268. *See* Sly et al., *supra* note 257. To understand why a benign business decision by a private company had such an adverse impact on national security, it is important to appreciate the individualized nature of the data revealed. Journalists, experts and others found ways to use the publicly available Strava data to identify individual users of the tracking service by name, along with the jogging routes they use in war zones such as Iraq and Afghanistan. *Id.*

269. *Id.* (describing a researcher who claims to have identified the names of 573 people who jog every morning around the parking lot of the headquarters of British intelligence, making it highly likely they work for the agency).

270. *Id.*

271. *Id.*

272. *Id.*

273. *Id.*

B. *A Data Surprise: Why the U.S. Missed the Data Aggregation Threat*

1. Focusing on Other Threats to Satellites

First, the U.S. military may have missed the aggregation threat because it was focused on threats to satellites of a different nature and type. The military was focused on threats from malicious actors, either nation states or organized terrorist groups. It was focused on threats of physical destruction to its own satellites. It was focused on threats of cyber operations against its military and commercially-owned satellites.

Most government policy statements regarding national security threats to satellites focus on malicious actors, either state actors or organized terrorist groups. Two recent examples illustrate this perspective. The National Air and Space Intelligence Center published *Competing in Space* in December 2018, in which it warned of the increasing capabilities of Russia and China in operating remote sensing satellites to support their military missions.²⁷⁴ The report stated that “China and Russia have the largest remote sensing satellite fleets outside the U.S.”²⁷⁵ The report includes graphics on the growing space launch capabilities of Russia and China²⁷⁶ and cites concerns about how the increasing use of dual-use technologies will “challenge U.S. ability to provide advanced warning of nefarious intentions or discern between peaceful and potential hostile activity.”²⁷⁷

Similarly, the U.S. military has been focused on threats of physical destruction to its own satellites and to other space objects. Such threats include satellite collisions, both accidental and intentional,²⁷⁸ as well as the debris fields created by such collisions. Recent examples of physical threats include China’s 2007 use of a ground-based anti-satellite missile

274. See generally NAT’L AIR & SPACE INTEL. CTR., *COMPETING IN SPACE* 6 (Dec. 2018),

<http://www.airforcemag.com/DRArchive/Documents/Competing%20in%20Space.pdf>.

275. *Id.* at 6.

276. *Id.* at 12–13.

277. *Id.* at 25; see also DAVID LIVINGSTONE & PATRICIA LEWIS, CHATHAM HOUSE, *SPACE, THE FINAL FRONTIER FOR CYBERSECURITY?*, at 9 (Sept. 2016), <https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf> (listing only threats from malicious actors).

278. See Brian D. Green, *Space Situational Awareness Data Sharing: Safety Tool or Security Threat?*, 75 A.F. L. REV. 39, 52–62 (2016).

to destroy one of its defunct weather satellites, Fengyun 1C.²⁷⁹ And in 2013, China launched another missile with the potential to strike targets in the geostationary orbit region.²⁸⁰ More recent efforts by China and Russia include efforts to develop anti-satellite missiles and counter-space directed-energy weapons and to establish networks of ground-based sensors to monitor and target the commercial and military satellites of other nations.²⁸¹

Finally, the U.S. military has been focused on the growing number and variety of cyber threats to satellite and space systems. These threats are not insignificant, and include threats to the space, user, link and ground segments of satellite systems.²⁸² Military planners and strategists worry about the real threat of hacking communications or navigational networks, targeting or hijacking control systems or specific electronics for missions, shutting down satellites, altering their orbits, “grilling” their solar cells through deliberate exposure to damaging radiation, redirecting or diverting the data the satellite transmits to someone other than its owner, operation or intended audience.²⁸³ The means are not unique to satellites and include hacking, command intrusion, payload control, denial of service, introducing malware to cause an abnormality in operations,²⁸⁴ spoofing, blinding, uplink and downlink jamming.²⁸⁵ In addition, older satellites, occasionally referred to as “space junk,” are particularly vulnerable to cyber operations.²⁸⁶

279. See William J. Broad & David E. Sanger, *China Tests Anti-Satellite Weapon, Unnerving U.S.*, N.Y. TIMES (Jan. 18, 2007), <https://www.nytimes.com/2007/01/18/world/asia/18cnd-china.html>; see also *Chinese Anti-satellite Test Creates Most Severe Orbital Debris Cloud in History*, ORBITAL DEBRIS Q. NEWS, Apr. 2007, at 2, 2–3 (Nat’l Aeronautics & Space Admin., Houston, Tex.), <https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv11i2.pdf>.

280. See Bill Gertz, *China Conducts Test of New Anti-Satellite Missile*, WASH. FREE BEACON (May 14, 2013, 1:46 PM), <https://freebeacon.com/national-security/china-conducts-test-of-new-anti-satellite-missile/>.

281. See COMPETING IN SPACE, *supra* note 274, at 20–21.

282. *Id.* at 18–19.

283. See Patricia Lewis & David Livingstone, *The cyber threat in outer space*, BULL. ATOMIC SCIENTISTS (Nov. 21, 2016), <https://thebulletin.org/2016/11/the-cyber-threat-in-outer-space/>; see also Green, *supra* note 278, at 25–26. Cyber warfare experts like Gen. John Hyten, commander of U.S. Strategic Command, have warned that China and Russia are developing “counter space capabilities” such as electronic jammers and advanced signal scramblers specifically to target U.S. military satellites. See Sandra Erwin, *Senior military official: Space secrets becoming harder to keep*, SPACENEWS (Jan. 30, 2018), <https://spacenews.com/senior-military-official-space-secrets-becoming-harder-to-keep/>.

284. See Green, *supra* note 278, at 26.

285. See COMPETING IN SPACE, *supra* note 274, at 19.

286. See Jan Kallberg, *Why older satellites present a cyber risk*, FIFTH DOMAIN (Dec. 28, 2018), <https://www.fifthdomain.com/opinion/2018/12/28/why-older-satellites-present-a-cyber-risk/> (describing the varied ways that malicious actors could take

In sum, the U.S. military has been focused, arguably appropriately so, on protecting its own satellites from physical or cyber attack by malicious actors. These threats should be considered and addressed by the U.S. military. However, the U.S. military needs to expand its focus to consider a new category of threats, those posed by the non-malicious aggregation of commercially-available satellite data.

2. A Disjointed and Cumbersome Regulatory Regime

A second reason the U.S. military failed to fully anticipate the threat posed by the aggregation of publicly available GPS data is due to the lack of a coherent legal regime on how to balance commercial interests and national security concerns in space. This is not a new problem. Since the initiation of space activities, the U.S. has attempted through legislation, regulation, and policy to balance national security concerns while promoting the peaceful commercial and research uses of outer space. The international community has attempted to strike a similar balance.

Any discussion of the international legal regime governing satellites will highlight five key authorities.²⁸⁷ Three of these authorities form the governing treaty law: the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space (the “Outer Space Treaty”),²⁸⁸ the 1972 Convention on International Liability for Damage Caused by Space Objects (the “Liability Convention”),²⁸⁹ and the 1975 Convention on Registration of Objects launched into Outer Space (the “Registration Convention”).²⁹⁰ Taken together, these three authorities attempt to balance the legitimate national security interests of individual nation states with the idea that “exploration and use of outer space . . . be carried out for the benefit and interests of all countries . . . and shall be the

advantage of older satellites relying on outdated hardware and software – occasionally from 1980s).

287. For an overview of the international laws governing remote sensing satellites, see *supra* Section VI.A. See also Hoversten, *supra* note 176, at 260–265.

288. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies art. 1, Jan. 27, 1967, 18.3 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].

289. Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187 [hereinafter Liability Convention] (requiring signatory states to accept absolute liability for damages caused by the state’s satellites to Earth and other satellites).

290. Convention on the Regulation of Objects Launched into Outer Space, Jan. 14, 1975, 29 U.S.T. 695, 1023 U.N.T.S. 15 [hereinafter Registration Convention] (requiring signatory states to maintain a national registry of objects it launches into space and report such information to the United Nations).

province of all mankind.”²⁹¹ The fourth authority, the 1987 Principles Relating to Remote Sensing of the Earth from Outer Space (the “UN Remote Sensing Principles”),²⁹² captured the “open skies” concept, which permits states to freely sense and distribute data from outer space without the consent of the sensed state.²⁹³ A final authority is Article 34 of the ITU Constitution,²⁹⁴ which gives states the right to cut off private telecommunications activities which threaten national security.²⁹⁵

The U.S. domestic legal regime attempts this same balancing act with regard to the use of remote sensing satellites. The first congressional finding in the Land Remote Sensing Policy Act of 1992 provided that “[t]he continuous collection and utilization of land remote sensing data from space are of major benefit in studying and understanding human impacts on the global environment, in managing the Earth’s natural resources, in carrying out national security functions, and in planning and conducting many other activities of scientific, economic, and social importance.”²⁹⁶ Likewise, the regulations governing the licensing of private remote sensing systems identify the following as a key purpose: to “[a]dvance and protect U.S. national security and foreign policy interests by maintaining U.S. leadership in remote sensing space activities, and by sustaining and enhancing the U.S. remote sensing industry.”²⁹⁷ This trend continues in the recently proposed, but not enacted, American Space Commerce Free Enterprise Act of 2017, which states: “It is the policy of the United States that, to the maximum extent practicable, the Federal Government shall take steps to protect the national security interests of the United States that do not involve regulating or limiting the freedoms of United States nongovernmental entities to explore and use space.”²⁹⁸ And finally, the recent Space Policy Directive-2, issued by President Donald

291. See Outer Space Treaty, *supra* note 288; see also Hoversten, *supra* note 176, at 261 (explaining how the Outer Space Treaty lays the foundation for principles of “common interest,” “freedom” and non-appropriation” in space).

292. G.A. Res. 41/65, Principles Relating to Remote Sensing of the Earth From Space (Dec. 3, 1986)[hereinafter UN Remote Sensing Principles].

293. See *id.* annex, at 2; see also Hoversten, *supra* note 176, at 260–265.

294. INT’L TELECOMM. UNION CONST. art. 34

295. See *id.* (“Member States also reserve the right to cut off, in accordance with their national law, any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency.”).

296. Land Remote Sensing Policy Act of 1992, Pub. L. No. 102-555, § 2(1), 106 Stat. 4163, 4163 (1992) (codified as amended at 51 U.S.C. ch. 601).

297. See 15 C.F.R. § 960.1 (2018).

298. See American Space Commerce Free Enterprise Act of 2017, H.R. 2809, 115th Cong. § 4(b) (2017). The bill passed out of the House of Representatives, and was referred to the Committee on Commerce, Science, and Transportation of the U.S. Senate in April 2018. See *Actions Overview H.R. 2809—115th Congress (2017-2018)*, CONGRESS.GOV, <https://www.congress.gov/bill/115th-congress/house-bill/2809/actions> (last visited June 20, 2019).

Trump in May 2018, provides: “It is therefore important that regulations adopted and enforced by the executive branch promote economic growth; minimize uncertainty for taxpayers, investors, and private industry; protect national security, public-safety, and foreign policy interests; and encourage American leadership in space commerce.”²⁹⁹

To protect the national security side of this scale, the U.S. government relies on a number of specific legal and policy authorities to restrict space activities that pose a threat to national security. These authorities include: the Remote Land Sensing Policy Act of 1992³⁰⁰ and subsequent amendments, codified at 51 U.S.C. Chapter 601; the implementing regulations at 15 C.F.R. Part 960; U.S. Commercial Remote Sensing Policy (dated April 25, 2003);³⁰¹ the National Space Policy of the United States (dated June 2010),³⁰² the U.S. Commercial Space Launch Competitiveness Act of 2015,³⁰³ which amended Title II of the Remote Land Sensing Policy Act; 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 (dated April 25, 2017);³⁰⁴ and Space Policy Directive-2 on “Streamlining Regulations on Commercial Use of Space” (dated May 24, 2018).³⁰⁵

While a full review of these authorities is beyond the scope of this article, we will focus on a few provisions with significant national security bite. As noted in Section VI *supra*, U.S. law requires owners and operators of private remote sensing space systems, including satellites, to secure a license from the U.S. Department of Commerce. The licensing authority

299. Space Policy Directive-2: Streamlining Regulations on Commercial Use of Space, 83 Fed. Reg. 24901, 24901 (May 30, 2018) [hereinafter Space Policy Directive-2]

300. Land Remote Sensing Policy Act of 1992, Pub. L. No. 102-555, 106 Stat. 4163 (1992).

301. REMOTE SENSING POLICY, *supra* note 39. The 2003 policy superseded Presidential Decision Directive 23, U.S. Policy on Foreign Access to Remote Sensing Space Capabilities (March 9, 1994), and urged the U.S. government to develop strong relationships with private sector entities in the remote sensing industry while ensuring appropriate protection of national security and foreign policy initiatives. *Id.*

302. NATIONAL SPACE POLICY, *supra* note 190.

303. U.S. Commercial Space Launch Competitiveness Act of 2015, Pub. L. No. 114-90, 129 Stat. 704 (2015).

304. 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 (April 25, 2017), <https://bit.ly/30b3bsQ> [hereinafter Remote Sensing MOU]. The 2017 MOU seems to replace an earlier MOU among these departments, dated February 2, 2000, although it does not expressly say so. See 15 C.F.R. pt. 960, app. 2 (2018).

305. Space Policy Directive-2, *supra* note 299.

is executed by NOAA's Commercial Remote Sensing Regulatory Affairs Office. Thus, the first national security checkpoint for remote sensing satellites comes in the license application process. The Department of Commerce's general licensing authority requires consultation with other appropriate U.S. government agencies, including the Department of the Defense when the license application is first submitted to ensure consideration of national security concerns. "No license shall be granted by the Secretary unless the Secretary determines in writing that the applicant will comply with . . . any . . . national security concerns of the United States."³⁰⁶ The nuts and bolts of the interagency review process that identifies, considers and assesses the national security interest is provided in the aforementioned Memorandum of Understanding.³⁰⁷

A second national security lever occurs when NOAA sets the initial conditions for the license. The regulations require that the licensee "operate its system in a manner that preserves the national security" and notes that the government may place limitations on the satellite's operational performance, "including, but not limited to, limitations on data collection and dissemination."³⁰⁸ In addition, the regulations require the licensee to maintain operational control of the satellite from a location within the U.S. with command override ability.³⁰⁹

A third national security check can occur either at the outset or during the license term. As part of the monitoring and compliance process, or due to changing national security circumstances, the government may require the licensee "to limit data collection and/or distribution by the system as determined to be necessary to meet significant national security or significant foreign policy concerns."³¹⁰ In addition, the government may, when "necessary to meet significant national security" interests, require the licensee to provide "unenanced restricted images on a commercial basis exclusively to the U.S. Government."³¹¹

306. 51 U.S.C. § 60121(b)(1) (2012 & Supp. 2017); *see also* 15 C.F.R. § 960.6(f) (2018) ("[n]o license shall be granted by the Secretary unless the Secretary determines, in writing, . . . that the granting of such license and the operation of the license and system by the licensee would be consistent with the national security interest . . . of the United States.").

307. Remote Sensing MOU, *supra* note 299.

308. 15 C.F.R. § 960.11(b)(1) (2018); *see also* 51 U.S.C. §§ 60122(b)(1), 60147(a) (2012 & Supp. 2017) ("The Secretary and the Landsat Program Management shall consult with the Secretary of Defense on all matters under this Act affecting national security. The Secretary of Defense shall be responsible for determining those conditions, consistent with this Act, necessary to meet national security concerns of the United States and for notifying the Secretary and the Landsat Program Management promptly of such conditions.").

309. 15 C.F.R. § 960.11(b)(2).

310. *Id.* § 960.11(b)(4).

311. *Id.*

A fourth and final national security touchpoint occurs in the reporting requirement. An important but often overlooked provision requires annual reports to Congress on various aspects of the licensing and enforcement provisions.³¹² This reporting provision requires the Secretary of Commerce to submit an annual report to the Committee on Commerce, Science, and Transportation of the U.S. Senate and the Committee on Science, Space, and Technology of the U.S. House of Representatives.³¹³ Among other items, the annual report must include a list of all applications for remote sensing licenses received in the previous calendar year, a list of all applications that resulted in a license for a remote sensing space system, and a list of all applications denied, as well as an explanation of why each application was denied, including any information relevant to the interagency adjudication process.³¹⁴

It is worth noting that the authorities listed above do not identify a specific type of national security threat, nor do they describe the scale, scope, or nature of the national security interest. Taken together, however, they provide a mechanism for the Department of Defense, and other national security entities, to identify and respond to national security concerns relating to the collection, use, access, and dissemination of imagery gathered by remote sensing satellites. More specifically, these provisions—in conjunction with the implementing regulations and executive branch policy statements³¹⁵—form the legal basis for the national security-related restrictions that the U.S. government places on privately-operated remote sensing satellites. These restrictions generally fall into four categories: (1) limitations on the operational performance of the satellite;³¹⁶ (2) requirements for reporting, monitoring, and compliance;³¹⁷ (3) limitations on foreign involvement in the U.S. remote sensing and satellite industry;³¹⁸ and (4) limitations on data collection and/

312. See 51 U.S.C. § 60126 (2012 & Supp. 2017).

313. *Id.* § 60126(a).

314. *Id.*

315. 15 C.F.R. pt. 960, app. 2 (2018) (“In consultation with affected agencies, limitations on commercial remote sensing systems will be imposed by the Secretary of Commerce when necessary to meet international obligations and national security and foreign policy concerns and will be in accord with the determinations of the Secretary of Defense and the Secretary of State and with applicable law”).

316. 15 C.F.R. § 960.11(b)(1) (2018).

317. See, e.g., 15 C.F.R. § 960.11(b)(3) (detailing a licensee’s reporting requirements).

318. See 15 C.F.R. § 960.8 (2018); see also 10 U.S.C. § 2274(a) (2012 & Supp. 2017). The National Defense Authorization Act for Fiscal Year 2010 amended 10 U.S.C. § 2274(a) by specifying when the Secretary of Defense can share SSA data, who can DOD share that data with, who must pay, and issues of civil and criminal immunity. See The National Defense Authorization Act for Fiscal Year 2010, Pub. L. No. 111-844, 123 Stat.

or dissemination, often referred to as “shutter control.”³¹⁹ This allows the U.S. government to prohibit images of a certain resolution, to prohibit imaging over a particular geographic location, and to restrict the clarity of the commercially available images when publicly released.³²⁰

C. *The Limits of the Current Regulations and New Developments*

Despite the seemingly broad reach of the national security restrictions on the collection and dissemination of satellite data, as described above, in practice they have limited application. The limits fall into three categories. First, a jurisdictional limit: the national security protections limit only U.S. companies subject to U.S. laws and regulations. While the regulations include restraints on foreign investment in U.S. satellite and remote sensing companies, there is nothing to prevent a foreign company from collecting, using, and sharing with others the data that the U.S. government identified as impacting national security interests.³²¹ Indeed, some have argued that the U.S. regulatory scheme actually accelerated the growth of satellite and remote sensing industries abroad. According to James Vedda, a senior policy analyst at Aerospace Corporation, “[a]ll you’ve really done is drive business to those foreign companies.”³²² The second category relates to criticisms of the inter-agency process for

2190. The Secretary of Defense has since delegated this authority to the Commander of the U.S. Strategic Command. See Green, *supra* note 278, at 63–64.

319. For an overview of these protections, see Hoversten, *supra* note 176, at 270–79. See also RICK HEIDNER, SHUTTER CONTROL: AN APPROACH TO REGULATION IMAGERY FROM PRIVATELY OPERATED RS SATELLITES (May 15, 2014), <https://bit.ly/2yNcRzc>; Sarah Scoles, *How The Government Controls Sensitive Satellite Data*, WIRED (Feb. 8, 2018), <https://bit.ly/2PYekZG>; Hamed Aleaziz, *Why Google Earth Can’t Show You Israel*, MOTHER JONES (June 10, 2011), <https://bit.ly/2YkobvM>. A notable example of geographic imaging restrictions occurred in 1997, when “Congress passed the annual National Defense Authorization Act, one section of which was titled, ‘Prohibition on collection and release of detailed satellite imagery relating to Israel.’ The amendment, known as the Kyl-Bingaman Amendment, permitted a U.S. government agency, NOAA’s Commercial Remote Sensing Regulatory Affairs, to regulate the dissemination of zoomed-in images of Israel.” Aleaziz, *supra* (emphasis omitted).

320. See 51 U.S.C. § 60121(b)(1) (2012 & Supp. 2017); see also 15 C.F.R. § 960.6(f) (2018). See also Scoles, *supra* note 319; National Defense Authorization Act for Fiscal Year 1997, Pub. L. No. 104-201, § 1064, 110 Stat. 2422, 2653 (1996) (Kyl-Bingaman Amendment). According to an October 2018 meeting of ACCRES, the U.S. currently limits imagery over Israel to “coarser than 2 meters GSD.” See Samira Patel, *NOAA’s Commercial Remote Sensing Regulatory Affairs*, NAT’L OCEANIC & ATMOSPHERIC ADMIN. 9 (Oct. 2018), <https://bit.ly/2Lz7MC6> (slide deck).

321. COMPETING IN SPACE, *supra* note 274, at 7.

322. See Scoles, *supra* note 319; see also COMPETING IN SPACE, *supra* note 274, at 6. The development of remote sensing satellite industry in other countries and the developments in imagery has reduced the ability of countries to perform sensitive military operations undetected.

seeking input and approving licenses. Complaints abound about long license processing times and a lack of transparency as to the reasons for license denials or limitations on data collection and dissemination. Similar complaints point to ineffective monitoring and compliance reports. A third limit is the outdated nature of the licensing scheme that is tasked with regulating an industry at the forefront of technological development and advancement. The current regulations were last updated in 2006, which was more than a decade ago and prior to the introduction of Apple's first iPhone.

Given these limits, it should come as no surprise that efforts at reform are coming from all quarters. In 2015, Congress passed the U.S. Commercial Space Launch Competitiveness Act of 2015 with the objective of facilitating a pro-growth environment for the development of a commercial space industry by encouraging private sector investment and creating more stable and predictable regulatory conditions.³²³ Recent legislative efforts have echoed this focus on encouraging private investment and improving the regulatory landscape, and have included the proposed American Space Commerce Free Enterprise Act of 2017³²⁴ and Space Frontier Act of 2019.³²⁵ Both included provisions aimed at shortening the duration of the license application process and providing greater clarity to license applicants.³²⁶

Indeed, the executive branch has been active as well. In May 2018, President Trump issued Space Policy Directive-2, titled "Streamlining Regulations on Commercial Use of Space."³²⁷ Section 3 of the directive tasks the Secretary of Commerce with reviewing—and possibly revising or rescinding—the licensing regime for commercial remote sensing systems,³²⁸ regulations which were adopted pursuant to Title II of the Land

323. See, e.g., U.S. Commercial Space Launch Competitiveness Act of 2015, Pub. L. No. 114-90, 129 Stat. 704 (2015).

324. American Space Commerce Free Enterprise Act, H.R. 2809, 115th Cong. (2018). This bill passed the House and was referred to the Senate in April 2018. See *Actions Overview H.R. 2809*, *supra* note 298. It would provide for a faster licensing timeline and put the burden on the government to prove why a company shouldn't get a license, rather than on a company for proving why it should. See also Scoles, *supra* note 319.

325. Space Frontier Act of 2019, S. 3277, 115th Cong. (2018). This bill passed the Senate but failed in the House. *Actions Overview S. 3277—115th Congress (2017-2018)*, CONGRESS.GOV, <https://www.congress.gov/bill/115th-congress/senate-bill/3277/actions> (last visited June 20, 2019).

326. DANIEL MORGAN, CONG. RESEARCH SERV., R45416, COMMERCIAL SPACE: FEDERAL REGULATION, OVERSIGHT, AND UTILIZATION, at 9 (2018), <https://fas.org/sgp/crs/space/R45416.pdf>.

327. See Space Policy Directive-2, *supra* note 299.

328. *Id.* at 24901-02

Remote Sensing Policy Act of 1992 (51 U.S.C. Chapter 601), and which were last updated in 2006, almost fifteen years ago.

Commerce Secretary Wilbur Ross wasted no time, and in June 2018, the department published an advance notice of proposed rulemaking.³²⁹ The comment period ran through the end of August 2018. According to ACCRES meeting minutes, NOAA received a whopping total of 10 comments during the 2 month period, with the comments generally focused on improving transparency in the licensing process, and transitioning from a “one size fits all” model.³³⁰ According the Advisory Committee on Commercial Remote Sensing, an entirely new set of regulations has been drafted and was sent to the Office of Management and Budget for review in late October 2018.³³¹ NOAA’s goal appears to be to publish final rules by the end of 2019.³³²

It is worth pausing a moment to consider the need for a comprehensive “regulation re-write”³³³ of the commercial remote sensing licensing scheme. The advance notice identified “ambiguities in the current regulatory regime, many of which were unforeseeable even just a few years ago” and offered the following specific examples:

- Dramatic increase in the number of license applications
- Increasing remote sensing capabilities in other countries
- Cubesat constellations
- Non-Earth imaging
- Satellite servicing
- Innovative systems capable of imaging in different spectral bands
- Live video broadcasting from space
- Venture capital investment, including significant amounts from foreign nationals and corporations
- New entrants to space markets
- Hosted payloads

329. Licensing Private Remote Sensing Space Systems, 83 Fed. Reg. 30592 (proposed June 29, 2018) (to be codified at 15 C.F.R. pt. 960); *see also* MORGAN, *supra* note 326, at 9.

330. 24th Meeting of the ACCRES Committee, *supra* note 195, at 3.

331. *See* Foust, *supra* note 203; 24th Meeting of the ACCRES Committee, *supra* note 195, at 3.

332. 24th Meeting of the ACCRES Committee, *supra* note 195, at 3.

333. *See* Patel, *supra* note 320, at 3.

- Increasing use of public-private partnerships
- Complex contractual relationships
- Satellite servicing missions, including proximity operations
- Ground station networks located in multiple countries with different regulatory regimes
- Launch vehicles imaging on orbit.³³⁴

It is interesting to note that the list did not mention the aggregation of geolocation data, the increasing number of sensor-based devices using commercial remote sensing data, such as IoT connected devices, or the advent of 5G networks. Nor were the Strava or Polar global activity maps referenced.

Not surprisingly, the private sector owners, operators and users of satellite data have not shied away from criticizing the current regulatory landscape. In 2016, DigitalGlobe CEO Walter Scott called for a rethinking of the regulatory regime for RS satellites, and a reset of the national security-commercial development balance, writing:

It's time for the U.S. government to rethink the basic premise underlying commercial remote sensing regulation. Instead of focusing solely on the risks, acknowledge the benefits that widely available U.S. commercial satellite imagery bring to national competitiveness. Acknowledge that commercially available satellite imagery has proven to be a great social benefit. Acknowledge that the U.S. space technology edge has eroded, and satellite imagery is now available from dozens of countries. Acknowledge that the feared dire risks from the commercial availability of satellite imagery never materialized. Acknowledge that U.S. industry has been very forward-leaning in protecting national security through self-policing. Acknowledge that the world has changed.³³⁵

To put it bluntly, the legal framework governing remote sensing satellites was complicated, jurisdictionally limited, and arguably ineffective in spotting national security interests before “sensored” wearable devices and IoT products became features of our daily lives; before commercial entities had the ability to aggregate geolocation and other data from multiple app-based sources; and before recent advances in enhanced imagery resolution, including increased pixelization. Thus, it

334. Licensing Private Remote Sensing Space Systems, 83 Fed. Reg. at 30592.

335. Walter Scott, U.S. Satellite Imaging Regulations Must Be Modernized, SPACENEWS (Aug. 29, 2016) <https://bit.ly/2He6sQV>.

may be an understatement to suggest that the regulatory regime is at a breaking point.

D. Data Aggregation Is a Persistent and Growing Concern

The national threat posed by commercial remote sensing data is not decreasing or going away. The number of remote sensing satellites operated by the United States public and private sectors is growing.³³⁶ Foreign states are similarly increasingly turning to remote sensing satellites.³³⁷ In 2008, there were 100 satellites with this capability; by 2018, there were 300 remote sensing satellites.³³⁸ The number of countries and multinational organizations that own or operate satellites is increasing due to the increasing commercialization of space and affordable space technology. Satellite ownership is no longer limited to a few space power countries. In 2018, more than 50 countries and multinational organizations owned or operated satellites.³³⁹ This persistent and growing challenge is one that will only increase with the advent of 5G technology. 5G will increase the number of satellites in orbit, expand the number of sensors gathering – and sharing – geolocation and other data. 5G networks will create civilian and military enterprises “teeming with constant rivers of data.”³⁴⁰ And to top it off, China and other nations are developing quantum computing satellites, with the capacity to capture and process vast amounts of imagery data.³⁴¹

Although the sections above examined how the U.S. military missed the threat posed by aggregation of geolocation data and their data-driven apps, it is important to note that not everyone in the U.S. government missed the potential national security threat. A 2017 GAO report identified “the geolocation capability of some IoT [Internet of Things] devices as a particular concern—specifically, how the location of troops or personnel could be revealed.”³⁴² However, this recognition did not prevent the Strava heatmap incident in January 2018. Nor did it prevent a similar incident

336. See *supra* Part III.C.

337. See COMPETING IN SPACE, *supra* note 274, and accompanying text.

338. See COMPETING IN SPACE, *supra* note 274, at 1.

339. See *id.* at 2.

340. See John P. Thomas, *5G From Space: 20,000 Satellites to Blanket the Earth*, TECHNOCRACY (Jan. 8, 2019), <https://bit.ly/2UEtpA9>.

341. See COMPETING IN SPACE, *supra* note 274, at 8.

342. See U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-668, INTERNET OF THINGS: ENHANCED ASSESSMENT AND GUIDANCE ARE NEEDED TO ADDRESS SECURITY RISKS IN DOD 18 (2017), <https://www.gao.gov/assets/690/686203.pdf>; see also Jacob Meschke, *Pentagon Severely Restricts Fitness Trackers After Strava Heatmap Scandal*, BICYCLING (Aug. 10, 2018), <https://bit.ly/2VtPMg7>.

with a global activity map prepared by Polar Fitness³⁴³ in July 2018. Using the data from Polar's Explore map, one could locate sensitive military sites and find a user's name and address, and users included military personnel from various military and intelligence agencies.³⁴⁴

Quite possibly, the significance of the national security information revealed by the heatmaps incidents may have provided the awakening moment – or at least more concrete recognition – by the U.S. national security establishment as to the scope and contours of a new type of threat: a threat posed not by the direct actions of malicious states or groups, but by simple commercial interests and a consumer desire for efficiency and convenience. “The rapidly evolving market of devices, applications and services with geolocation capabilities presents a significant risk to the Department of Defense personnel on and off duty, and to our military operations globally,” said Pentagon spokesman Army Col. Robert Manning III on August 6, 2018.³⁴⁵ Thus, the question going forward is how will the U.S. stem the “rising river of digital metadata” in a way that protects national security interests, and relatedly, how will it prevent malicious actors from dipping into that river of data.³⁴⁶

IX. RECOMMENDATIONS

The recommendations offered below are nascent in scope and require further consideration and development. However, the broad brushstrokes seem appropriate as we work to bridge the legal and regulatory chasms in this area while grappling with the powerful and transformative role that remote sensing data plays in commercial, individual, and military endeavors. We make these recommendations as a launching point for further discussions and as a framework to begin development and eventual implement of proposed policy and regulatory changes. We do so with full understanding that any act that interferes with or disrupts the availability, integrity and reliability of satellites and satellite data will have significant impacts on our civilian and military realms.

343. See Andrew Liptak, *Polar Fitness Suspends its Global Activity Map After Privacy Concerns*, THE VERGE (July 8, 2018), <https://bit.ly/2KW02LG>.

344. See *id.*

345. See Jim Garamone, *New Policy Prohibits GPS Tracking in Deployed Settings*, U.S. DEP'T OF DEF. (Aug. 6, 2018), <https://bit.ly/2Gz1vAy>.

346. See Patrick Turner, *Strava's Just the Start: The US Military's Losing War Against Data Leakage*, DEF. ONE (Jan. 31, 2018), <https://bit.ly/2vqCemM>.

Number 1: Revise the International Space Object Registry to require more detailed and publicly available information about data collection, use, aggregation, and dissemination.

We start with our most practical recommendation. Space object registries should add requirements mandating that the owner/operator: (1) identify the data that will be collected; (2) specify the intended use for the data; (3) identify the entities with which the data will be shared or disseminated; and (4) make that information transparent and publicly available, wherever feasible. The lack of transparency in the current international framework makes it difficult to anticipate, appreciate, or respond to the privacy and national security risks presented by aggregation of satellite generated data.

The U.N. maintains a Register of Objects Launched into Outer Space, more colloquially referred to as the Space Object Register.³⁴⁷ The Register was initially “established as a mechanism to aid the United Nations Committee on the Peaceful Uses of Outer Space in its discussions on the political, legal and technical issues concerning outer space” and has become “a means of identifying which States’ bear international responsibility and liability for space objects.”³⁴⁸ To be included in the Register, the owner or operation must complete the “Registration Information Submission Form,” available on the United Nations Register of Objects Launched into Outer Space website, hosted by United Nations Office for Outer Space Affairs (UNOOSA) website.³⁴⁹ The two-page form requires only limited information on the launching state, the designator, the date and territory or location of the launch, the basic orbital parameters, any change of status, and the “general function of the space object.”³⁵⁰ There is no requirement to provide information as to the specifics of the satellite’s function, or the type, use or dissemination of the data it will gather.³⁵¹

347. See *United Nations Register of Objects Launched into Outer Space*, U.N. OFFICE FOR OUTER SPACE AFFAIRS, <https://bit.ly/2atzZrq> (last visited June 20, 2019).

348. See *id.*

349. See *Registration Information Submission Form*, U.N. REGISTER OF OBJECTS LAUNCHED INTO OUTER SPACE (Jan. 1, 2010), <https://bit.ly/2UVRmIh>.

350. See *id.*

351. See *id.*

Number 2: Revise the U.S. licensing regime for commercial remote sensing space objects to make the full licenses publicly available absent significant concerns about national security or international obligations.

The U.S. licensing regime for private remote sensing space systems requires a significantly greater level of detail,³⁵² including applicant contact information (including foreign owners and lenders), launch segment information, space segment information; ground segment information; as well as other information. In particular, the application requirements are quite robust and include: “system data collection and processing capabilities”; “data distribution and archiving plans”; “plans for providing access to or distributing the unenhanced data generated by the system”; “a description of the plan for the sale and distribution of such data”; and a “method for making the data available to governments whose territories have been sensed.”³⁵³

The U.S. regulations require the *license applicant* to include specific information in the application about data collection, use and dissemination. Similarly, the regulations require the *U.S. government* to include specific information in the approved license regarding data collection, use and dissemination. However, the detailed information about data collection, use and sharing generally is not available *to the public*. Instead, the regulations require only that public summaries of current commercial remote sensing licenses be posted on the Commercial Remote Sensing Regulatory Affairs website.³⁵⁴ The summaries tend to be less than one page in length, and lack detailed information about how the satellite will collect, use, or share data.

For example, there are three public license summaries available for DigitalGlobe on the CRSRA website. Each summary provides information about the launch dates, orbital parameters, and image resolution.³⁵⁵ However, the public summaries contain no information about the use or dissemination of the imagery data being collected. There is one interesting statement in the public summary for the GeoEye Imagery Collection System: “Due to U.S. licensing restrictions, commercial customers may

352. See Filing Instructions and Information, 15 C.F.R. pt. 960, app. 1 (2018).

353. See *id.*

354. See *NOAA Licensees*, NAT’L OCEANIC & ATMOSPHERIC ADMIN. (Apr. 17, 2019), <https://bit.ly/2J04Bk3>.

355. See *GeoEye-1 License*, *supra* note 90; *Private Remote Sensing System License Public Summary* (DigitalGlobe WorldView system), NAT’L OCEANIC & ATMOSPHERIC ADMIN. (2006), <https://bit.ly/2XKj87x>; *Summary of Private Land Remote-Sensing Space System License* (DigitalGlobe), NAT’L OCEANIC & ATMOSPHERIC ADMIN. (2017), <https://bit.ly/2Pu5QJt>.

only receive imagery from GeoEye-1 at half-meter or greater ground resolution.”³⁵⁶

The need for classification is understandable in many instances, however, there are also instances when the full license can be made publicly available, and in those instances, it should be. Commerce Secretary Ross identified streamlining the regulatory process and providing greater transparency to license applicants as priorities. That transparency should be extended to the public so they understand how the data being collected and shared—or sold—by the license applicant may affect their privacy.

Number 3. Ensure that aggregation of satellite geolocation data is on the agenda of international dialogues about cyber governance and international security frameworks.

In 2018, the U.N. celebrated the 50th anniversary of the first United Nations Conference on the Exploration and Peaceful Uses of Outer Space. In the coming years, the Liability Convention and Registration Convention will also celebrate 50 years. It is an opportune moment to ensure that international dialogues about the use of outer space, satellites and remote sensing include discussions of data aggregation, privacy interests and national security.

Future international dialogue should build upon the recommendations of the U.N. Group of Governmental Experts on Transparency and Confidence-building Measures in Outer Space Activities as expressed in its concluding report,³⁵⁷ published in July 2013. Other international entities particularly well-poised to consider the issues discussed in this article include the U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, and the U.N.’s Working Group on the “Space2030” Agenda.

Historically, these working groups and discussions have focused on armed conflict scenarios in space and the weaponization of space objects to achieve military ends. It is critical that these discussions move beyond the armed conflict and use of force paradigms to appreciate the significant threat posed, not by malicious nation state actors or rouge terrorist organizations, but by the simple business decisions of private sector entities with access to incredible amounts of satellite sourced data.

³⁵⁶ *GeoEye-1 License*, *supra* note 90.

³⁵⁷ G.A. Ses. 68/189, Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities (July 29, 2013), <https://undocs.org/A/68/189>.

Number 4: Ensure that U.S. policymakers understand the scope and scale of threats posed by the satellite-smart device information nexus and amend the relevant U.S. authorities to correct the disconnect between constitutional privacy, domestic electronic surveillance laws, and satellite regulation.

Despite tremendous press coverage of the Strava incident, and recent legislative efforts to revisit the balance between commercial interests and national security,³⁵⁸ the U.S. government has failed to appreciate the complexities posed by the commercial use, aggregation and sale of satellite data. The Summary of the 2018 National Defense Strategy did not include the word “satellite” or the term “remote sensing,” nor did the 2018 Summary of the Department of Defense Cyber Strategy.³⁵⁹ The 2018 National Cyber Strategy used the word satellite only once. In a section on improving space cybersecurity, the strategy provided: “The Administration is concerned about the growing cyber-related threats to space assets and supporting infrastructure because these assets are critical to functions such as positioning, navigation, and timing (PNT); intelligence, surveillance, and reconnaissance (ISR); satellite communications; and weather monitoring.”³⁶⁰ The December 2018 “Competing in Space” report, prepared by the National Air and Space Intelligence Center, did discuss satellites and remote sensing, however, it focused on physical and cyber threats from malicious actors, notably China and Russia.³⁶¹ The Competing in Space report did not discuss the Strava or Polar incidents, nor did it discuss how to address the cresting wave of remote sensing data related to IoT and 5G.

We do not mean to suggest the U.S. government is willfully ignoring the problem. It is not. After the Strava and Polar incidents, the Pentagon responded to the specific threat posed by the use of wearable devices with geolocation features by servicemembers. On August 3, 2018, the Pentagon issued a DOD Policy Memo that announced: “Effective immediately, [Defense Department] personnel are prohibited from using geolocation features and functionality on both non-government and government-issued devices, applications, and services while in locations designated as operational areas [.]”³⁶² The memo directs prompt

358. See *supra*, Part VIII, section B.3., See also generally MORGAN, *supra* note 326.

359. See generally U.S. DEP’T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY (2018), <https://bit.ly/2OCwui5>.

360. EXEC. OFFICE OF THE PRESIDENT, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 10 (Sept. 2018), <https://bit.ly/2xrQ0XX>.

361. See generally COMPETING IN SPACE, *supra* note 274.

362. See Memorandum from the Deputy Sec’y of Def. to the Chief Mgmt. Officer of the Dep’t of Def. et al., Use of Geolocation-Capable Devices, Applications, and Services

development of geolocation risk management guidance and training and mandates an update of the annual Cybersecurity Awareness training to educate DoD personnel the risks posed by geolocation capabilities embedded in devices and apps.³⁶³ Similarly, the GAO identified these specific concerns in a July 2017 report, noting that “the geolocation capability of some IoT [Internet of Things] devices as a particular concern—specifically, how the location of troops or personnel could be revealed.”³⁶⁴

The Pentagon’s prohibition, however, does not address the actual problem. It fails to grasp the satellite-smart device information nexus, and it bizarrely assumes that individuals are capable of controlling “geolocation features and functionality” on a myriad of highly sophisticated smart devices and apps. While the Pentagon policy changes and the GAO reports are important developments, we are urging a larger rethinking and recognition of the problem by the U.S. government. Specifically, the U.S. government must take concrete actions to understand and address the threats discussed in this paper.

First, on the policy side, those working on future National Defense Strategy and Cyber Strategy documents must examine and address the security challenges and civil liberties concerns posed by remote sensing satellites. Likewise, given the President’s recent space-related directives,³⁶⁵ we anticipate a new U.S. Space Policy document, designed to replace the 2010 policy, is in the works. The new space policy document must address the privacy and national security concerns posed by data aggregation from remote sensing satellites. In a similar vein, NOAA’s Advisory Committee on Commercial Remote Sensing (ACCRES) must broaden its perspective to embrace both commercial interests *and* privacy and civil liberties concerns. According to its website, ACCRES “evaluates economic, technological, and institutional developments relating to commercial remote sensing” and serves as “a forum for the discussion of issues involving the relationship between industry activities and

(Aug. 3, 2018), <http://bit.ly/2EiQovh> [hereinafter Geolocation Memo]; *see also* Garamone, *supra* note 345; Meschke, *supra* note 342.

363. *See* Geolocation Memo, *supra* note 362; *see also* Garamone, *supra* note 345. According to news stories, the DoD is also considering limiting the apps that servicemembers can use, mandating devices that show which apps allow third-party siphoning and banning personal smartphones in the Pentagon, similar to the ban at CIA headquarters. The DoD’s Defense Information Systems Agency, which serves as the military’s IT department, is charged with leading this effort. *See* Tara Copp, *Fitbits and Fitness-tracking Devices Banned for Deployed Troops*, *Military Times* (Aug. 6, 2018), <https://www.militarytimes.com/news/your-military/2018/08/06/devices-and-apps-that-rely-on-geolocation-restricted-for-deployed-troops/>.

364. *See* Meschke, *supra* note 342.

365. *See National Space Council Directives*, OFFICE OF SPACE COMMERCE (2019), <https://bit.ly/2Pu6TZI>.

Government policies, programs, and regulatory requirements.”³⁶⁶ The threat posed by aggregated satellite data to privacy and national security must be part of its wheelhouse, and ACCRES’s committee membership must include privacy and domestic surveillance experts.

Second, regulatory change is needed. A November 2018 CRS asked whether and how the commercial space licensing process could be made simpler, timelier, and more transparent.³⁶⁷ The response offered is telling:

Congressional attention to this question has focused, in large part, on the process for interagency consultation on commercial remote sensing licenses. The challenge for that process is balancing industry’s need for timeliness and transparency with the government’s need to meet national security and foreign policy objectives. The rapidly advancing capabilities of foreign government and commercial satellites make identifying the appropriate balance more difficult, because if sensitive imagery can be obtained elsewhere, prohibiting U.S. companies from providing it may have few security benefits.³⁶⁸

Nonetheless, the on-going 15 C.F.R. 960 “re-write” of the commercial remote sensing licensing scheme should try to strike the balance correctly. The new rules should address the rapid and mind-binding technological developments that have exposed ambiguities in the current regulatory scheme. In the addition, the new regulations should: make the full license application and approved license publicly available to the greatest extent possible; extend the annual congressional reporting requirement, which is set to sunset in 2020; add an unclassified executive summary, available to the public, as part of the annual report to Congress; revise the license application requirements to specify data type, collection method, whether and how the data will be aggregated with other sources (if known), and how the data will be sold or disseminated.

Third, specific changes are needed in the legislative realm. The disconnect between satellite regulation and domestic privacy and electronic surveillance law must be addressed by Congress. Comprehensive overhaul of the U.S. electronic privacy and surveillance statutory scheme is long overdue. As we continue to move rapidly into 5G platforms, smart cities, and our interconnected IoT universe, the satellite-smart device information nexus must be part of the regulatory and policy

366. See *Advisory Committee on Commercial Remote Sensing*, NAT’L OCEANIC & ATMOSPHERIC ADMIN., <https://bit.ly/2Vj8U12> (last updated Oct. 11, 2018).

367. See generally MORGAN, *supra* note 326.

368. *Id.* at 24.

framework. Satellites, generally, and commercial remote sensing, specifically, provide the technical underpinnings and data that enable these systems to function. But satellite-smart device data aggregation is not part of our domestic privacy and electronic surveillance data framework. The satellite-smart device information nexus must be part of our data law framework. Here are two immediate steps to be taken: the FY20 National Defense Authorization Act drafting process is well underway: in its funding, planning and response, the NDAA must address the threat posed by aggregation of satellite-smart device information nexus. Next, Congress should to reintroduce and pass the Geolocation Privacy and Surveillance Act or similar legislation to establish a legal framework for when and how geolocation information can be accessed and used.

X. CONCLUSION

*Over time, therefore, the modern “use” of satellites has evolved into a “reliance” upon them, which has graduated into a “dependence,” and eventually generated a “vulnerability.” Potential adversaries, aware of the technology patterns of the United States (and others), have come to appreciate the suggestion that satellites may now be the Achilles heel of the American civilian economy and its mighty military apparatus.*³⁶⁹

This article is an initial effort to frame, understand, and address the vulnerabilities posed to individual privacy, civil liberties, and national security by the satellite-smart device information nexus. The Strava incident, by no means an isolated example, provided a moment of recognition for scholars and policymakers as to the scope and contours of a new type of threat: a threat posed not by the direct actions of malicious states or groups, but by commercial interests and unaware consumers and policy makers. Thus, the question going forward is: how will the U.S. and the international community respond?

ⁱ Anne Toomey McKenna is co-author of *Wiretapping & Eavesdropping: Surveillance in the Internet Age*, 3rd Ed., and *Jones on Evidence*, 7th Ed., both of which have been cited in published opinions by numerous federal and state courts, along with other articles and posts. McKenna is currently writing a new *Cyberlaw* casebook to be published by Wolters Kluwer in 2019. With funding from the National Security Agency (NSA), McKenna just completed development of *Cyberlaw: Policy & Operations*, a course that NSA has offered nationwide to college/graduate students and professionals across the U.S. McKenna also served as the Principal Legal Consultant for the Justice Department’s Office of Community Oriented Policing Services on the use of UAVs by domestic law enforcement. In addition to her publications and academic positions, McKenna is a trial attorney licensed in federal and state courts in Maryland and the District of Columbia. with more than two decades of

369. See Koplow, *supra* note 259.

federal and state court litigation experience in cyber, privacy, electronic surveillance, cellular law, workplace privacy, data practices and data breach, website policies, geolocation tracking, online content and speech, and online torts. McKenna is a frequent print, television, and radio media contributor, she is a regularly invited speaker on privacy and cyber-related subjects, and she has served on and moderated dozens of legal and cyber/privacy panels. McKenna continues to consult with government and the private sector about AI and machine learning, wiretapping, computer and cellular searches, geolocation tracking, and unmanned aerial vehicles (UAVs). McKenna teaches Information Privacy Law, Cyberlaw, Civil Procedure, Evidence, and Media Law.

ⁱⁱ Amy Gaudion's scholarship focuses on cybersecurity, national security law, and civilian-military relations. She leads the law school's national security and cybersecurity programs. Gaudion established and leads an annual cybersecurity working group simulation in collaboration with the U.S. Army War College. She is the author of *Defending Your Country . . . and Gender – Legal Challenges and Opportunities Confronting Women in the Military*, in *Women, Law and Culture: Conformity, Contradiction and Conflict* (Jocelynnne A. Scutt ed., 2016) (Palgrave Macmillan). Her work has appeared in scholarly journals as well as *The New York Times* and *The Daily Beast*. Gaudion has served on and moderated numerous panels examining the impact of technology on the legal framework governing national security and intelligence, including *Cybersecurity and Data Privacy: Equifax, the VEP, and CISA*; *iPhone vs. the FBI: Government Surveillance in the Post-Snowden Era*; *The Constitutionality and Consequences of America's Use of Drones and the NSA Spying Program*; and *After Bin Laden: Stuxnet, Drones and the New Middle East*. She has appeared on WITF's Smart Talk and WHY's Radio Times. She served as a legal advisor to *World on Trial*, a public television and multimedia project that aims to elevate public awareness of important human rights issues and the international treaties that govern state conduct. Gaudion teaches courses in national security law, cybersecurity law and policy, and constitutional law.

ⁱⁱⁱ Jenni L. Evans' research encompasses tropical cyclones from genesis to decay, extratropical transition [ET], or landfall, as well as developing new methodologies for satellite tracking of systems that may become tropical cyclones. The impacts of climate change on tropical cyclones [TCs] and other organized tropical convective systems are also key components of her research. Evans was one of a small group of scientists who developed a new understanding of extratropically transitioning tropical cyclones, systems such as Hurricane Sandy of 2012. Evans collaborated on developing a framework for mapping the structural evolution of cyclonic storms, the Cyclone Phase Space (CPS). The CPS is used in operations, including at the US National Hurricane Center. In her recent research, Evans has employed a variety of novel statistical methodologies for (1) physically-based partitioning of ensemble forecasts of tropical cyclones; and (2) developing a metric for tropical cyclogenesis activity in climate change simulations. Evans is a Fellow of the American Meteorological Society (AMS) and served on its Council from 2005 to 2008. She co-chaired the World Meteorological Organisation (WMO) 8th Intergovernmental Workshop on Tropical Cyclones (Seoul, Republic of Korea; December 2014) and has served for over a decade as the Lead Meteorologist for the Professional Team assisting the Florida Commission on Hurricane Loss Projection Methodology. Other current and former professional service include the US Weather Research Program Science Steering Committee, Science Steering Committee for the US THORPEX Pacific Asian Regional Campaign, Advisory Board for the NOAA/NSF Developmental Testbed Center, Editor of Monthly Weather Review and Associate Editor of Weather and Forecasting. The tools of Evans' research and work include observational diagnostics; statistical analyses and modeling of observations, simulations and reanalyses; and dynamical modeling. Evans

is reliant upon and uses an array of satellites, satellite technologies, and satellite data in her research and work.