(Slip Opinion)

Application of the Pen-Trap Statute and the Wiretap Act to Unmanned Aircraft System Detection Technologies

The Pen-Trap Statute, 18 U.S.C. § 3121 *et seq.*, prohibits the "use" of a pen register or trap and trace device only if that device has first been "attached or applied" to a "telephone line or other facility." The term "facility" includes neither the end-user devices that transmit or receive a communication, nor the "electronic or other impulses" transmitted and received by those end-user devices.

Under the Wiretap Act, a radio communication may be intercepted under 18 U.S.C. § 2511(2)(g)(i) if it does not fall within one of the statutory categories listed in 18 U.S.C. § 2510(16). A non-radio electronic communication may be intercepted under 18 U.S.C. § 2511(2)(g)(i) if it is transmitted by an electronic communication system that incorporates elements that make the communication's contents easily obtainable by the general public.

Detecting unmanned aircraft systems through the use of acoustic, electrooptical and infrared, and radar technology systems generally does not violate either the Pen-Trap Statute or the Wiretap Act.

Detecting unmanned aircraft systems through the use of radiofrequency detection systems does not violate the Pen-Trap Statute so long as the radiofrequency detection device or process is not attached or applied to a telephone line or other facility.

Using radiofrequency detection systems to conduct spectrum monitoring or to intercept remote identification broadcasts generally does not violate the Wiretap Act. Whether the use of radiofrequency detection systems to intercept other communications violates the Wiretap Act must be determined on a case-by-case basis.

November 24, 2026

MEMORANDUM OPINION FOR THE COUNSEL TO THE PRESIDENT

Drones—also known as unmanned aircraft systems ("UAS")—present an unparalleled opportunity to "reshap[e] the future of aviation." Exec. Order No. 14307, § 1, 90 Fed. Reg. 24727, 24727 (June 6, 2025). From leisure to logistics, agriculture to emergency response, UAS are changing the way Americans live, do business, and are protected by their government. *Id.* But as with any advancement in technology, America's enemies have sought to exploit the proliferation and availability of UAS. "More than 95 countries," including foreign adversaries, "reportedly operated some sort of uncrewed military aircraft in 2021."[1] UAS are also

[1] Kelley M. Sayler & Michael E. DeVine, Cong. Rsch. Serv., R47188, *Unmanned Aircraft Systems: Roles, Missions, and Future Concepts* at 23 (July 18, 2022); *see also*

increasingly employed by malevolent non-state actors and criminal organizations.[2] The Department of War has therefore assessed UAS as "pos[ing] the most significant threat" to overseas "personnel, facilities, and assets," and as presenting an increasing threat within the United States.[3]

In response, Congress has authorized certain federal departments, as well as state, local, tribal, and territorial ("SLTT") law-enforcement and correctional agencies, to conduct a variety of counter-UAS ("C-UAS") operations. *See* 6 U.S.C. § 124n (governing Department of Homeland Security, Department of Justice, and SLTT operations); 10 U.S.C. § 130i (governing Department of War operations[4]); *id.* § 6227 (governing Department of Energy operations); 50 U.S.C. § 3515a (governing Central Intelligence Agency operations). When operating within these statutory authorities, authorized personnel are exempted from various criminal statutes—including those prohibiting the destruction of aircraft or aircraft facilities, 18 U.S.C. § 32; unauthorized access of computer systems, *id.* § 1030; interception of electronic communications, *id.* § 2511; installation or use of pen registers and trap-and-trace devices, *id.* § 3121; interference with satellite operations, *id.* § 1367; and aircraft piracy, 49 U.S.C. § 46502. *See, e.g.*, 6 U.S.C. § 124n(a).[5] But using

---

Wilson Beaver & Ka'Von Johnson, Heritage Foundation, *Countering the Drone Threat: Steps for the U.S. Military* 2–3 (2025), https://perma.cc/XY4E-FPS9.

[2] Cole Black, *The Houthi Model—Non-State Actors and Multi-Drone Capabilities*, Small Wars J. (Dec. 30, 2025), https://perma.cc/K3XC-V354; *see also* Vanda Felbab-Brown, *How Mexican Cartels Are Using Drones, Now and in the Future*, Brookings Inst. (Feb. 18, 2026), https://perma.cc/59UT-88GL; Daniel M. Gettinger, Cong. Rsch. Serv., R48477, *Department of Defense Counter Unmanned Aircraft Systems: Background and Issues for Congress* at 1, 27 (Mar. 31, 2025); Matt Rivers et al., *'Threat from Above': Prisons Face Escalating Threat from Drones*, ABC News (Dec. 12, 2025) https://perma.cc/HE6F-8AEE; *see generally* Beaver & Johnson.

[3] Press Release, Department of War, DoD Announces Strategy for Countering Unmanned Systems (Dec. 5, 2024), https://perma.cc/2NQE-RFP3.

[4] We have not been asked, and therefore do not consider, the Department of War's ability to conduct C-UAS operations under the President's Article II authority.

[5] These statutory authorities do not relieve compliance with the Communications Act or other federal regulations governing access to the radiofrequency spectrum. *See, e.g.*, 47 U.S.C. § 301 (licensing and authorization); *id.* § 303 (interfering devices); *id.* § 333 (jamming); *id.* § 605 (unauthorized transmissions). We understand that the Federal Communications Commission ("FCC") is addressing compliance requirements to facilitate the implementation of the SAFER SKIES Act, Pub. L. No. 119-60, tit. LXXXVI, 139 Stat. 1938 (2025). *See generally* FCC, *Counter-UAS* (Aug. 18, 2026), https://perma.cc/MN8K-PWJM.

these statutory authorities remains subject to certain limitations. For instance, the C-UAS statute addressing SLTTs limits the types of technologies that they may employ. *Id.* § 124n(d)(2)(A)(iii). And information-sharing amongst federal agencies and between the federal government and SLTTs is restricted except under certain circumstances. *See, e.g.*, *id.* § 124n(e)(4)–(5).

You have asked us to consider whether the use of acoustic, electro-optical and infrared ("EO/IR"), radar, and radiofrequency-detection systems outside the C-UAS statutory authorities violates the Pen-Trap Statute or Wiretap Act. We conclude that the use of such UAS-detection systems does not generally violate either statute. Subject to certain limitations and qualifications identified in this opinion, federal and SLTT personnel may deploy such systems without relying on the C-UAS statutory authorities.[6] But we caution that the use of radiofrequency-detection systems that obtain the contents of UAS communications may violate the Wiretap Act, except under the circumstances described herein.

Part I provides an overview of UAS technology and describes the four categories of UAS-detection systems that you requested we consider. Part II explains the legal frameworks of the Pen-Trap Statute and Wiretap Act. Part III applies those statutes to the UAS-detection system categories.

I.

A.

A UAS is "an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system." 49 U.S.C. § 44801(12). It is composed of four main elements: an unmanned aircraft, a control component, the payload, and the communication architecture.

---

[6] Courts have long held that the Supremacy Clause of the United States Constitution protects federal officers "from state prosecutions" and private suits under state law "for actions reasonable and necessary in the discharge of their federal responsibilities." *Wyoming v. Livingston*, 443 F.3d 1211, 1217 (10th Cir. 2006). But SLTT personnel acting outside the scope of 6 U.S.C. § 124n(a) may be subject to state eavesdropping laws and statutes governing the use of pen registers and trap and trace devices. *See* Anne Toomey McKenna & Clifford S. Fishman, *Wiretapping and Eavesdropping* §§ 3:56–3:106, 4:24 (Dec. 2025) ("*Wiretapping and Eavesdropping*"). This opinion does not interpret those laws or provide guidance to SLLT personnel who may be subject to them.

The first element is the unmanned aircraft itself. Federal law defines an unmanned aircraft as "an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft." *Id.* § 44801(11). Unmanned aircraft come in a variety of shapes and sizes. *See* Joshua Brungardt & Kurt Carraway, *The "System" in UAS*, in *Introduction to Unmanned Aircraft Systems* 57, 58–60 (R. Kurt Barnhart et al. eds., 3d ed. 2021).

The second element is the payload, which is the sum of accessories that the unmanned aircraft carries. *See* Siva Sivamani Ganesh Kumar & Abhishek Gudipalli, *A Comprehensive Review on Payloads of Unmanned Aerial Vehicle*, 27 Egyptian J. Remote Sensing & Space Scis. 637, 638–39 (2024); *see also* Brungardt & Carraway at 64–67. Payloads may include explosives, drugs, and contraband. *See generally* Felbab-Brown; Black; Rivers et al. But the typical payload includes "[s]ensors and video cameras." Kumar & Gudipalli, 27 Egyptian J. Remote Sensing & Space Scis. at 638. These onboard devices may record data or transfer that data in real-time to terrestrial, airborne, spaceborne, or maritime receivers. Drone Warfare, *Counter-UAS 101 – Radio Frequency (RF) Drone Detection* § 1.1 (2025), https://perma.cc/HK9W-BBVT ("Drone Warfare, *RF Drone Detection*"). The unmanned aircraft's payload should not be confused with the data it transmits, which are sometimes called payload communications. *See* 47 C.F.R. § 88.5. For clarity, we use the terms "payload" to describe the accessories carried by the unmanned aircraft and "communications" to describe data transmitted over various data links.

The third element is the control component. *See* Brungardt & Carraway at 60–61. Unmanned aircraft can be divided into those that are remotely piloted and those that are automatic or autonomous. *Id.* Remotely piloted unmanned aircraft rely on "an interface used by the remote pilot to control the flight path of" the unmanned aircraft, known as a ground control station. 14 C.F.R. § 107.3; *see also* Brungardt & Carraway at 61. By contrast, automatic or autonomous aircraft rely on pre-programmed coding to execute missions using onboard GPS, inertial navigation, or other technologies. *See* Drone Warfare, *RF Drone Detection* § 4.2; Brungardt & Carraway at 60–61.

The fourth element—and the most important for purposes of this opinion—is the communication architecture. *See* Brungardt & Carraway at 62–64; *see generally* Saeed M. Khan, *Unmanned Aircraft Systems (UAS) Communications*, in *Introduction to Unmanned Aircraft Systems* at 291,

291–319. UAS typically employ "multiple [radiofrequency] links operating simultaneously." Drone Warfare, *RF Drone Detection* § 1.1. The command and control ("C2") link "carries pilot inputs from the controller to the [unmanned aircraft] and returns telemetry data about battery status, GPS position, altitude, and system health." *Id.* Other links can transmit and receive video and other data from payload systems. *See id.* Unmanned aircraft flying near the ground control station typically use "line-of-sight" radiofrequency communications that primarily operate within the 2.4 GHz, 5.8 GHz, and 900 MHz Industrial, Scientific, and Medical ("ISM") radiofrequency bands. *See id.* §§ 1.1–1.2; RF Essentials, *What Frequency Bands are Used for Drone Command and Control Links and What are the Range Limitations?*, https://perma.cc/8Q65-3RVD; Nathan Maresch, *Command and Control*, in *Introduction to Unmanned Aircraft Systems* at 321, 326.[7] Operations at greater distances—known as "over the horizon" or "beyond-line-of-sight" C2—"rely on satellite communication systems," Linell A. Letendre, *Lethal Autonomous Weapon Systems: Translating Geek Speak for Lawyers*, 96 Int'l L. Stud. 274, 283 (2020), or "an intermediary relay radio link," Marco Hernandez et al., *Security Strategies for Unmanned Aircraft Systems Networks*, 2023 IEEE Int'l Conf. on Commc'ns Workshop on CyberNet 996, 996; *see generally* Brungardt & Carraway at 64. Automatic or autonomous systems do not require a C2 link, but they may still require satellite links for navigation or for delivery of communications during flight. *See* Drone Warfare, *RF Drone Detection* § 4.2; Maresch at 336.[8]

---

[7] Common radiofrequency technologies include Wi-Fi (standard or enhanced), Lightbridge Communication Protocol, and OcuSync Communication Protocol. Driss Aouladhadj et al., *Drone Detection and Tracking Using RF Identification Signals*, 23 Sensors, no. 17, 2023, at 3–6. Fiberoptic-controlled UAS can also be used for short-range missions. Drone Warfare, *RF Drone Detection* § 4.2; *see generally* Alex Braszko, *Fiber Optic Drones: Posing a Significant C-UAS Challenge*, U.S. Army (Aug. 12, 2025), https://perma.cc/W8YM-M4HL.

[8] Communications transmitted via radiofrequency may be conveyed using modulation techniques. Many UAS "hop" among radiofrequencies over a defined radiofrequency band. *See* Jonathan A. Messier, *"Too Legit to Quit:" Free Speech Clause Protection for Frequency Hopping Spread Spectrum Broadcasters*, 9 Pitt. J. Tech. L. & Pol'y 1, 29–31 n.111 (2008); *see also* Drone Warfare, *RF Drone Detection* § 1.3; Brungardt & Carraway at 64. These communication-architecture frameworks may be combined with additional protocols such as Advanced Encryption Standard to secure the connection. *See* Hernandez et al., 2023 IEEE Int'l Conf. on Commc'ns Workshop on CyberNet at 998–99.

B.

Since 2012, the Secretary of Transportation has "develop[ed] a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system." FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332(a)(1), 126 Stat. 11, 73. As part of that plan, FAA has issued numerous regulations. *See generally* 14 C.F.R. pts. 48, 89 & 107. Two are pertinent here.

First, apart from limited circumstances, *see id.* § 89.101, FAA requires all UAS to broadcast remote identification during flight operations, *see id.* §§ 89.105, 89.110, 89.115. "In its most basic form, remote identification can be described as an electronic identification or a 'digital license plate' for UAS." *Remote Identification of Unmanned Aircraft*, 86 Fed. Reg. 4390, 4396 (Jan. 15, 2021). Once every second, the aircraft must broadcast its serial number, location, velocity, and emergency status as well as the location of its control station or its takeoff location. *See* 14 C.F.R. §§ 89.305, 89.310(h)(5), 89.315. That broadcast must be on a "non-proprietary broadcast specification and us[e] radio frequency spectrum" such as Bluetooth or Wi-Fi channels, which makes the information widely available to anyone in range of the signal. *Id.* § 89.310(g)(1); *see also* 86 Fed. Reg. at 4427.

Second, FAA requires most unmanned aircraft to be registered. *See* 14 C.F.R. §§ 48.15, 107.13; *see also id.* §§ 48.15(b), 107.1(b) (listing exceptions). To register, one must provide specified contact information, the UAS make or model, and the UAS's remote-identification serial number. *See id.* § 48.110. This registration system allows FAA and law enforcement to correlate the remote-identification broadcast with the UAS owner. *See* 86 Fed. Reg. at 4393.

C.

C-UAS technology can be divided into two classes: detection systems and mitigation systems. *See Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies*, 91 Fed. Reg. 41466, 41466 (July 6, 2026) (describing the SAFER SKIES Act's "two-tiered structure for detection and warning operations and for mitigation operations"). Detection systems "detect, track, or identify UAS operating in the airspace." Cybersecurity and Infrastructure Security Agency, *Unmanned Aircraft System Detection Technology Guidance*

for Critical Infrastructure 2 (2025), https://perma.cc/K2TD-HP74 ("CISA Guidance"). Mitigation systems, by contrast, may "destroy, take over, or down (i.e., mitigate) a UAS through electronic, kinetic, and/or other means." *Id.* We address here only detection systems, which can be grouped into four categories: acoustic, EO/IR, radar, and radiofrequency.

1.

Drones make noise. "No rotary-wing aircraft can fly without displacing air, and therefore no drone is truly silent." Drone Warfare, *Counter-UAS 101 – Acoustic Drone Detection* § 1.2 (2026), https://perma.cc/8NDH-ASEW ("Drone Warfare, *Acoustic Drone Detection*"). Because the "harmonic structure" of that displaced air varies by a drone's "blade geometry, loading, and operational state," the harmonic structure creates a sort of "fingerprint" for the UAS. *Id.* § 2.1. Acoustic UAS-detection systems employ "groups of specially tuned microphones," CISA Guidance at 5, to listen for and identify that acoustic fingerprint using various acoustic analysis techniques, *see* Drone Warfare, *Acoustic Drone Detection* §§ 4–5; Ulzhalgas Seidaliyeva et al., *LiDAR Technology for UAV Detection: From Fundamentals and Operational Principles to Advanced Detection and Classification Techniques*, 25 Sensors, no. 9, 2025, at 3. If the harmonic structure is matched to a fingerprint in the database by multiple microphones, the system can not only identify the make and model of UAS but also estimate its location and velocity. *See* CISA Guidance at 5; Drone Warfare, *Acoustic Drone Detection* §§ 1.2, 6.

2.

EO/IR detection systems use the visible and infrared light of the electromagnetic spectrum. EO/IR systems come in passive or active varieties.

In their most basic form, passive EO/IR systems use camera arrays to collect visible light. This light is produced into a continuous sequence of images, which are analyzed for the distinct movement of drones across frames. *See* CISA Guidance at 6. Slightly more complex thermal-imaging systems can detect a drone's "thermal signature[] . . . against the cold sky or ambient background." Drone Warfare, *Counter-UAS 101 – Electro-Optical and Infrared Detection* § 2.1 (2026), https://perma.cc/79YS-CNS7. Thermal cameras passively capture infrared electromagnetic radiation and then perform an analysis much like their electro-

optical counterparts. *See* Kumar & Gudipalli, 27 Egyptian J. Remote Sensing & Space Scis. at 638.

By contrast to these passive EO/IR technologies, light detection and ranging ("LiDAR") is an active EO/IR technology. LiDAR "uses the concepts of reflected light and precise timing to determine the distance between objects." Seidaliyeva et al., 25 Sensors at 4. The system consists of a transmitter that emits near-infrared laser pulses and a receiver that absorbs the reflected light. *See id.* at 5. "The distance between the transmitter and reflector is [then] calculated using th[e] laser's period of flight." Kumar & Gudipalli, 27 Egyptian J. Remote Sensing & Space Scis. at 638. LiDAR can not only capture "quick and precise" one- and two-dimensional data, *id.*, but it can also "capture precise high-resolution [three-dimensional] spatial data," Seidaliyeva et al., 25 Sensors at 4.

3.

Radio detection and ranging—commonly known as radar—is currently the primary means of UAS detection. *See* Drone Warfare, *Counter-UAS 101 – Radar Drone Detection* (2026), https://perma.cc/Y62F-MT2T ("Drone Warfare, *Radar Drone Detection*"); *see also* Airsight, *Drone Detection Radar: How It Works, Costs & Types*, https://perma.cc/TQ5Q-B5QF ("Airsight, *Drone Detection Radar*"). Radar uses "very brief bursts of radio energy, which move at the speed of light" and are "reflected off a target, and then returned as an echo." Kumar & Gudipalli, 27 Egyptian J. Remote Sensing & Space Scis. at 638. Like EO/IR detection, radar comes in passive and active varieties.

Passive radar systems do not themselves emit any electro-magnetic waves. Rather, they exploit radio waves transmitted from sources such as FM radio, television, and cellular networks. Drone Warfare, *Radar Drone Detection* § 3. These systems consist of two receivers—one that captures the unadulterated radio waves from the transmission source and one that captures those radio waves' reflection off airborne objects. *See id.* By comparing the original waves with the reflected waves, the system can identify the airborne object's presence, range, and velocity. *See id.*

Active radar, by contrast, consists of a transmitter and receiver. The transmitter emits either a pulsed or continuous stream of radio waves, which reflect off airborne objects and are collected by the receiver. *See*

Airsight, *Drone Detection Radar*; Drone Warfare, *Radar Drone Detection* § 2. The system determines the object's distance by the time delay between transmission and reception; it determines the object's velocity by a phenomenon known as the Doppler shift;[9] and it determines the object's bearing based on the angular position of the system at the time of detection or, in the case of electronically scanned systems, from beam-steering or monopulse processing. *See* Airsight, *Drone Detection Radar*. The emergence of advanced radar technology has allowed systems to distinguish unmanned aircraft from other small airborne objects such as birds. *See* Seidaliyeva et al., 25 Sensors at 3; Drone Warfare, *Radar Drone Detection* § 1.3.

4.

Passive radiofrequency detection involves sensing and analyzing the radio waves that UAS emit. Spectrum monitoring systems collect the radio emissions used to control a given UAS and analyze the signal's "frequency patterns, modulation schemes, and timing sequences." Drone Warfare, *RF Drone Detection* § 1.1. The system then compares this "signature" against known UAS signatures stored in a large dataset, or "library," to distinguish UAS "signals from other [radiofrequency] activity in the environment." *Id.* § 1.3; *see also* Joint Interagency Task Force 401, *Counter-UAS Operations: Safeguarding Freedoms & Preserving Privacy* *1 (2026), https://perma.cc/SSY9-KD77 ("JIATF 401 Guidance"). Through this analysis, "[m]ultiple sensors working in concert can triangulate positions, providing latitude, longitude, and in some cases altitude for both" the unmanned aircraft and the ground control station. Drone Warfare, *RF Drone Detection* § 1.1. This process occurs *without* acquiring the "substance, purport, or meaning" of the UAS communication. 18 U.S.C. § 2510(8); *see also* JIATF 401 Guidance at *2.

Other radiofrequency-detection systems take advantage of widespread compliance with FAA regulations that require UAS to broadcast their remote identification. *See* 14 C.F.R. §§ 89.105, 89.110. Because the broadcast operates on standard Wi-Fi or Bluetooth channels and does not

[9] The Doppler effect is the "chang[ing] in the observed frequency of a wave . . . when the source and observer are in motion relative to each other." *The American Heritage College Dictionary* 420 (4th ed. 2002). This is the same effect that makes the pitch of an emergency siren change for an observer as an ambulance gets closer.

employ security protocols, remote-identification communications are "available to most personal wireless devices within range of the broadcast." FAA, *Executive Summary: Final Rule on Remote Identification of Unmanned Aircraft (Part 89)*, at 1 (2020), https://perma.cc/D72Z-XJED ("FAA Rule Summary"). UAS-detection systems can therefore scan for these broadcasts, which provide the user with the location of the UAS ground control station or that of the UAS's takeoff location, as well as the location, velocity, and emergency status of the unmanned aircraft. *See* AirSight, *Detecting Drones with Remote ID, RF, and DF Sensors*, https://perma.cc/G8UL-HAKP; *see also* 14 C.F.R. §§ 89.305, 89.315.

Finally, some radiofrequency-detection systems engage in protocol decoding or other forms of signal analysis. *See* Drone Warfare, *RF Drone Detection* § 1.3. Like spectrum monitoring, these systems scan for the unique radiofrequency properties of UAS communication links. But unlike spectrum monitoring, these systems seek to acquire the contents of the UAS communication by demodulating the signal, decoding the protocol, and parsing the data. *See id.*

II.

Congress has enacted statutes that enable certain federal and SLTT law-enforcement officers and correctional agencies to undertake C-UAS actions to enforce the law and to protect people, places, and assets. *See* 6 U.S.C. § 124n. Subject to applicable law, law-enforcement officers and correctional agencies may also undertake C-UAS actions outside the § 124n framework. But acting within the statutory authorities confers relief from certain federal laws that might otherwise prohibit C-UAS actions.[10]

Two of those laws are relevant here: the Pen-Trap Statute and the Wiretap Act. Each statute addresses a different aspect of electronic communications, including those involved in UAS detection. To understand their distinctive roles, consider an analogy to a letter. The transmission (the envelope) contains both "dialing, routing, addressing, and signaling" information associated with a wire or electronic communication

[10] The "[n]otwithstanding" clauses of 6 U.S.C. § 124n(a), 10 U.S.C. §§ 130i(a), 6227(a), and 50 U.S.C. § 3515a(a) are sometimes called "statutory reliefs" because they were designed to relieve the relevant governmental agencies of obligations that federal laws might otherwise impose.

("DRAS") (the name, address, and zip code of the sender and recipient in our analogy) and the communication itself (the letter). The Pen-Trap Statute sets forth the processes by which the government can obtain DRAS information. *See* Orin S. Kerr, *Computer Crime Law* 618 (3d ed. 2013) ("Kerr, *Computer Crime Law*"). The Wiretap Act regulates the government's ability to acquire communicative contents. *See id.* at 579–80. We address each statute in turn, as both are potentially applicable to UAS-detection technologies deployed outside the C-UAS statutory authorities.

A.

Title III of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, 1868 ("ECPA")—commonly known as the "Pen-Trap Statute"—prohibits any person from recording, decoding, or capturing DRAS information "without first obtaining a court order" as detailed by the statute. ECPA sec. 301(a), § 3121(a), 100 Stat. at 1868; *see id.* §§ 301–303, 100 Stat. at 1868–73 (codified as amended at 18 U.S.C. § 3121 *et seq.*). Although we are unaware of any "criminal prosecutions under the Pen-Trap Statute"—against users of C-UAS technology or anyone else, Josh A. Goldfoot, *The Pen-Trap Statute and the Internet*, 6 Va. J. Crim. L. 1, 5 (2018)[11]—the President must "take Care that the Laws be faithfully executed," U.S. Const. art. II, § 3, including the Pen-Trap Statute. That duty extends to "tak[ing] care that his subordinates faithfully comply with the law." *Congressionally Mandated Notice Period for Withdrawing from the Open Skies Treaty*, 44 Op. O.L.C. 184, 192 (2020). We therefore must ensure that law-enforcement officials engaged in C-UAS activities outside the statutory C-UAS authorities comply with the Pen-Trap Statute.

1.

Historically, a "pen register" "referred to a device that record[ed] telephone numbers dialed" by passing "electric current through an electro-

[11] This is likely because citizens who surveil communications inevitably "collect content, not just non-content," and "are therefore prosecuted under the Wiretap Act," which carries more severe penalties than the Pen-Trap Statute. Goldfoot, 6 Va. J. Crim. L.at 5; *see also* 18 U.S.C. § 2511(4)(a) (providing for up to five years' imprisonment under the Wiretap Act, a fine, or both).

magnet," which "deflected a pen that would then mark a strip of paper." Goldfoot, 6 Va. J. Crim. L. at 8; *see also* William A. Claerhout, *The Pen Register*, 20 Drake L. Rev. 108, 109–10 (1970) (explaining the mechanics of a pen register). "Trap and trace" devices "record[ed] the phone numbers of phones used to dial a targeted phone line." Goldfoot, 6 Va. J. Crim. L. at 8; *see also In re Application of the U.S. for an Ord. Authorizing the Installation of a Pen Reg. or Touch-Tone Decoder & a Terminating Trap*, 610 F.2d 1148, 1152–53 (3d Cir. 1979) (explaining the mechanics of a trap-and-trace device). When the Pen-Trap Statute was enacted, courts had long held that the DRAS information these devices collect falls outside the scope of the Fourth Amendment. *See Smith v. Maryland*, 442 U.S. 735, 745–46 (1979). Because the information obtained by pen-trap devices "reveal[s] little in the way of 'identifying information'" and is "'voluntarily conveyed'" to a third party—such as a telephone company or internet-service provider—the service subscriber has no reasonable expectation of privacy in such information. *Carpenter v. United States*, 585 U.S. 296, 314 (2018) (first quoting *Riley v. California*, 573 U.S. 373, 400 (2014); and then quoting *United States v. Knotts*, 460 U.S. 276, 281 (1983)).[12]

In enacting the Pen-Trap Statute, Congress sought to restrict private and public actors' "use of pen registers and associated trap-and-trace devices" (together, "pen-trap devices"), Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz*,* Smith*, and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1, 14 (2016), while simultaneously facilitating government surveillance by requiring third parties to assist in the installation of court-ordered pen-trap devices, *see* Goldfoot, 6 Va. J. Crim. L. at 11. Congress thus commanded that "no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title." 18 U.S.C. § 3121(a). The only exceptions given are for "provider[s] of electronic or wire

[12] *See also Chatrie v. United States*, 609 U.S. 605, 632–35 (2026) (explaining how the Court distinguished the information involved in *Carpenter* from that involved in *Smith*); *United States v. Soybel*, 13 F.4th 584, 592–94 (7th Cir. 2021) (rejecting a post-*Carpenter* challenge to pen-trap orders for IP address data and noting a developing agreement among the circuit courts); Rich Haglund, *Applying Pen Register and Trap and Trace Devices to Internet Communications: As Technology Changes, Is Congress or the Supreme Court Best-Suited to Protect Fourth Amendment Expectations of Privacy*, 5 Vand. J. Ent. & Tech. L. 137, 141–43 (2003) (explaining why there is no reasonable expectation of privacy in DRAS information associated with internet communications).

communication service[s]" (also known as a "communication service provider"[13]), *id.* § 3121(b), and emergency or similar situations, *id.* § 3125(a)(1)(A)–(C). Violators may be punished with a fine, imprisonment for up to one year, or both. *Id.* § 3121(d).

The USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 216(c)(2)–(3), 115 Stat. 272, 290 (codified at 18 U.S.C. § 3127(3)–(4)) ("PATRIOT Act"), amended the telephone-based definitions of "pen register" and "trap and trace device" "to include Internet technology." Goldfoot, 6 Va. J. Crim. L. at 8–9; *see also* Kerr, *Computer Crime Law* at 619–20. These amendments had the effect of abstracting away from historical pen registers or trap-and-trace devices. Now, the "definitions are functional. They apply to any 'device or process which' *does* certain things." Goldfoot, 6 Va. J. Crim. L. at 10. "Pen register" now "means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication[14] is transmitted." 18 U.S.C. § 3127(3). "'[T]rap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." *Id.* § 3127(4). Returning to our analogy of a letter, a pen register reads the recipient's address, whereas a trap-and-trace device reads the envelope's return address. A device that reads both functions is simultaneously a pen register and a trap-and-trace device. *See* Computer Crime and Intellectual Property Section, Department of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 153–54 (3d ed. 2009) ("DOJ, *Searching & Seizing*").

2.

Having examined the Pen-Trap Statute's prohibition in context, we conclude that it applies only to the use of devices or processes

[13] The Pen-Trap Statute adopted the Wiretap Act's definition of "electronic communication service," *see* 18 U.S.C. § 3127(1), which is "any service which provides to users thereof the ability to send or receive wire or electronic communications," *id.* § 2510(15).

[14] The Pen-Trap Statute adopted the Wiretap Act's definitions of "wire communication" and "electronic communication." *See* 18 U.S.C. § 3127(1) (cross-referencing 18 U.S.C. § 2510).

"attached or applied" to a "telephone line or other facility." 18 U.S.C. § 3123(b)(1)(A), (C). Importantly, the "facility" to which a pen-trap device can be "attached or applied" does not include end-user devices that transmit or receive a communication. *Id.*; *see* Dan C. Marinescu, *Cloud Computing: Theory and Practice* 176 (2013); Goldfoot, 6 Va. J. Crim. L. at 39 (concluding that Congress did not intend the Pen-Trap Statute to apply to consumer devices).[15] Nor does it include the "electronic or other impulses" transmitted and received by those devices. *See* 18 U.S.C. § 3127(4).[16]

a.

The Pen-Trap Statute's core prohibition contains two verbs: "install" and "use." *Id.* § 3121(a). Although both words are "capable of many meanings," each "gathers meaning from the words around it" and may be "known by the company it keeps . . . to avoid the giving of unintended breadth to the Acts of Congress." *Jarecki v. G.D. Searle & Co.*, 367 U.S. 303, 307 (1961); *see also Yates v. United States*, 574 U.S. 528, 543 (2015) (plurality opinion).

"Use" is the broader of the two terms. It means "to employ for some purpose; put into service; make use of." *The Random House Dictionary*

[15] We arrived at a similar conclusion in our 1993 analysis of caller-identification technology. *See* Memorandum for Renee Licht, Acting General Counsel, Federal Communications Commission, from Walter Dellinger, Assistant Attorney General, Office of Legal Counsel, *Re: Interstate Caller Identification Services—Applicability of Federal Wiretap Statutes and Authority of the Federal Communications Commission to Preempt State Laws Inconsistent with Proposed Federal Communications Policy* at 8–9 (Oct. 28, 1993) ("Dellinger Memorandum"). We there concluded that a telephone subscriber's caller-identification display was not a trap-and-trace device because the trap and trace occurred on the communication service provider's system. *Id.* at 8. Once the communication service provider completed the trap and trace, it sent the information to the caller-identification display. *Id.* The caller-identification display thus acted as an end-user device, not as a trap-and-trace device. *Id.*; *see also Sparshott v. Feld Ent., Inc.*, 311 F.3d 425, 432 (D.C. Cir. 2002) (arriving at the same conclusion and collecting cases).

[16] The federal government initially advised that that "using [radiofrequency] capabilities to detect and track UAS by monitoring the communications passed between a UAS and its ground control station *may* implicate the Pen[-]Trap Statute." Department of Justice et al., *Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems* 2 (2020), https://perma.cc/7XM7-G7D5 (emphasis added). We now provide a more fulsome analysis of the Pen-Trap Statute to better delineate which technologies do and do not violate the statute.

of the English Language 2097 (2d ed. 1987) ("*Random House 1987*"). Interpreting that word "in view of [the statute's] structure and of the physical and logical relation of its many parts," Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 167 (2012), we observe that "use" is paired with "install" throughout the Pen-Trap Statute. That pairing is disjunctive in § 3121, so to "install" *or* "use" a pen-trap device violates the statute; one need not both install *and* use such a device to be found guilty of an offense. But "conjunctions are versatile words" that "can work differently depending on context." *Pulsifer v. United States*, 601 U.S. 124, 151 (2024). And the remainder of the Pen-Trap Statute uses the verbs "install" and "use" conjunctively. The statute authorizes an attorney for the United States to apply for an order "authorizing or approving the *installation and use* of a" pen-trap device. 18 U.S.C. § 3122(a)(1) (emphasis added); *see also id.* § 3125(a)(1) (authorizing the emergency "*installation and use*" of a pen-trap device (emphasis added)). Upon such application, "the court shall enter an ex parte order authorizing the *installation and use* of a" pen-trap device, so long as the government attorney has certified that "the information likely to be obtained by such *installation and use* is relevant to an ongoing criminal investigation." *Id.* § 3123(a)(1) (emphases added). And a communication service provider, "landlord, custodian, or other person" must assist in the "*installation and use*" of a pen-trap device. *Id.* § 3124(a)–(b) (emphasis added); *see also id.* § 3123(a)(3)(A) (permitting the government to "*install*[] *and us*[*e*]" its own pen-trap device on a communication service provider's "packet-switched data network" (emphasis added)). This repetitive formulation shows that "iteration is obviously afoot." *Moskal v. United States*, 498 U.S. 103, 120 (1990) (Scalia, J., dissenting). That iteration indicates a close logical association between installation and use, such that a pen-trap device is the kind of device that must be "installed" before it can be "used." *Cf.* Goldfoot, 6 Va. J. Crim. L. at 36–38 (arriving at the same conclusion by construing the definitions of "pen register" and "trap and trace device"). This reading is bolstered by the fact that Congress spilled significant ink to ensure that law enforcement had access to the "information, facilities, and technical assistance necessary to accomplish" that installation. 18 U.S.C. §§ 3123(b)(2), 3124(a)–(b).

To "install" means "to place in position or connect for service or use." *Random House 1987* at 987; *see also Webster's Third New International*

Dictionary 1171 (1993 ed.) ("*Webster's Third 1993*") (defining "install" as "to set up for use or service"). But this raises the question: Installed on what? We conclude that a pen-trap device must be "attached or applied" to a "telephone line or other facility." 18 U.S.C. § 3123(b)(1)(C). This interpretation is supported by statutory structure and history, as well as by the purpose of the Pen-Trap Statute.

To begin, statutory structure makes clear that a pen-trap device must be installed on a "telephone line or other facility." As noted above, the statute repeatedly refers to the "install[ation] and use" of a pen-trap device, *see, e.g.*, *id.* §§ 3121(c), 3122(a)(1), 3123(a)(1), but it never explicitly identifies the object to which those verbs apply. Statutory context provides the answer. Section 3123(b) explains that a court order authorizing the use of a pen-trap device must specify "the identity, if known, of the person to whom is leased or in whose name is listed the *telephone line or other facility* to which the [pen-trap device] is to be *attached or applied*." *Id.* § 3123(b)(1)(A) (emphases added). The order must also specify "the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the *telephone line or other facility* to which the [pen-trap device] is to be *attached or applied*." *Id.* § 3123(b)(1)(C) (emphases added). It must additionally direct the owner or lessor of the "*line or other facility* to which the [pen-trap device] is *attached or applied*" not to disclose the pen-trap device's existence or the existence of the investigation. *Id.* § 3123(d)(2) (emphases added). Section 3124 likewise requires those with access to the "appropriate *line or other facility*" to assist with the pen-trap device's installation. *Id.* § 3124(b) (emphasis added); *see also id.* § 3124(a). And finally, § 3126 requires that the Attorney General report to Congress "the number and nature of the *facilities* affected" by pen-trap orders. *Id.* § 3126(4) (emphasis added). The statute therefore indicates that a pen-trap device must be "attached or applied" to a "telephone line or other facility."

Statutory history further supports this conclusion. *See Reconsidering the Application of the Hyde Amendment to the Provision of Transportation for Women Seeking Abortions*, 49 Op. O.L.C. __, at *9 (July 11, 2025) (observing the importance of statutory history in discerning the meaning of words or phrases that have "several plausible definitions" (quoting *United States v. Hansen*, 599 U.S. 762, 775 (2023))); *Application of 10 U.S.C. § 191 and Section 8044 of Pub. L. No. 118-47 to the*

Defense Innovation Unit and Strategic Capabilities Office, 50 Op. O.L.C. __, at *17 (Apr. 22, 2026) ("*Application of Section 191*") (recognizing that statutory history "forms part of the context" in which we interpret statutory provisions (alteration adopted) (quoting Scalia & Garner at 256)). When ECPA was first enacted, a pen-trap device could only be installed on a telephone line. *See* Claerhout, 20 Drake L. Rev. at 109–10; *In re U.S. Application*, 610 F.2d at 1152–53; *see also* Dellinger Memorandum at 6; *Wiretapping and Eavesdropping* §§ 4:6, 4:8. And the statute reflected that limitation.[17]

The PATRIOT Act amended the Pen-Trap Statute to embrace modern communication technologies, particularly those involving the internet. PATRIOT Act § 216(b)(2), (c)(2)–(3), 115 Stat. at 289–90; *see also Wiretapping and Eavesdropping* § 4:17; Orin S. Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 626 (2003). In doing so, Congress expanded the definitions of "pen register" and "trap and trace device" to include devices or processes that record, decode, or capture DRAS information associated with a wire or electronic communication. PATRIOT Act § 216(c)(2)–(3), 115 Stat. at 290. Pen-trap devices, as newly defined, could now be installed on things other than telephone lines. But Congress did not eliminate the statute's original language or create a free-standing prohibition on the collection of DRAS information. Congress instead reinforced the statute's focus on infrastructure that facilitates the transmission of wire and electronic communications. Specifically, Congress amended §§ 3123 and 3124 to recognize that a pen-trap device could be installed on a telephone line "*or other facility*." *Id.* § 216(b)(2)–(3), (c)(6), 115 Stat. at 289–90 (emphasis added). And it clarified that a pen-trap device could not only be "attached" to such lines and facilities, but also that it could be "applied" to such physical and digital infrastructure, *id.* § 216(b)(2), 115 Stat. at 289–90, in recognition that a pen-trap

[17] *See* ECPA sec. 301(a), §§ 3123(b)(1)(A), (C), 3124(b), 100 Stat. at 1869–71 (requiring court orders to identify, if known, the "person to whom is leased or in whose name is listed," and the "physical location" of, the "*telephone line* to which the pen register or trap and trace device is to be *attached*," and requiring communication service providers, landlords, custodians, and other persons to assist the installation of a pen-trap device on "the appropriate *line*" (emphases added)); *id.* sec. 301(a), § 3126(3), 100 Stat. at 1871 (defining "pen register" as a device that "records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the *telephone line* to which such device is *attached*" (emphases added)).

device could now be a "process," such as a software program, Goldfoot, 6 Va. J. Crim. L. at 9–10. The intimate connection between the Pen-Trap Statute's expanded definitions and the other PATRIOT Act amendments indicates that pen-trap devices are the type of technology that must be "attached or applied" to a "telephone line or other facility."

An interpretation limiting the Pen-Trap Statute's prohibition to the installation of pen-trap devices on telephone lines or other facilities accords with the scheme Congress sought to enshrine. The Pen-Trap Statute was Congress's response to two Supreme Court cases. In *United States v. New York Telephone Co.*, 434 U.S. 159, 166 (1977), the Court held that pen registers were not governed by the Wiretap Act. Two years later, the Court held that information obtained by pen-trap devices was not protected by the Fourth Amendment. *See Smith*, 442 U.S. at 745–46. This information was therefore left constitutionally and statutorily unprotected. The Pen-Trap Statute closed the gap by providing modest protections to such information while facilitating the government's ability to obtain this information. *See* Bellovin et al., 30 Harv. J.L. & Tech. at 14–15; Goldfoot, 6 Va. J. Crim. L. at 7–8, 11; Haglund, 5 Vand. J. Ent. & Tech. L. at 140. But an interpretation that extends § 3121's prohibition to *any* DRAS information would sweep well beyond this modest goal. *See* Kerr, 97 Nw. U. L. Rev. at 631 (noting that DRAS information "has traditionally received little if any protection in communications networks such as the postal system and the telephone"). Indeed, it "could lead to the anomalous result of a court finding criminal culpability for the collection of [DRAS] information that would have been justified if content information had been collected instead. Worse, a court might rule a single act both legal, with respect to the content captured, and illegal, with respect to non-content." Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. Ill. L. Rev. 1417, 1480. And such an interpretation would be particularly anomalous considering that the PATRIOT Act sought to *expand* governmental access to DRAS information. *See* Bellovin et al., 30 Harv. J.L. & Tech. at 16–17; Kerr, 97 Nw. U. L. Rev. at 637–38.

b.

A close reading of the Pen-Trap Statute reveals that a "facility" to which a pen-trap device can be "attached or applied" does not include

end-user devices—*i.e.*, the originator's equipment that transmits a communication or the equipment employed by the intended recipient to receive the communication. *Cf.* 18 U.S.C. § 2510(5)(a) (excluding "any telephone or telegraph instrument, equipment or facility, or any component thereof" that is used to connect to a communication service provider's facilities in the ordinary course of business).

"Facility" means "something designed, built, installed, etc., to serve a specific function affording a convenience or service." *Random House Webster's Unabridged Dictionary* 690 (2d ed. 2001) ("*Random House 2001*").[18] But when describing the "facility" to which a pen-trap device must be attached or applied, the Pen-Trap Statute consistently pairs "facility" with "telephone line." *See, e.g.*, 18 U.S.C. §§ 3123(b)(1)(A), 3123(b)(1)(C), 3123(d)(2), 3124(b). "Under the familiar interpretive canon *noscitur a sociis*, 'a word is known by the company it keeps.'" *Dubin v. United States*, 599 U.S. 110, 124 (2023) (quoting *McDonnell v. United States*, 579 U.S. 550, 568–69 (2016)). "Facility," in this context, must therefore be interpreted in relation to "telephone line" to avoid giving "facility" "unintended breadth," *id.* at 124–25 (quoting *McDonnell*, 579 U.S. at 569); *see also Fischer v. United States*, 603 U.S. 480, 486–88 (2024). A telephone line is the infrastructure that facilitates a wire or electronic communication between two or more end-user devices (such as the telephones themselves). But a telephone line does not include the end-user devices that transmit or receive the call. Interpreted in this light, a "facility" to which a pen-trap device may be attached or applied must likewise be infrastructure (physical or digital) that facilitates the transmission of a wire or electronic communication between end-user devices.[19] And like a telephone line, "facility" in this context

---

[18] *See also Webster's Third New International Dictionary* 812–13 (2002 ed.) ("*Webster's Third 2002*") (defining "facility" as "something (as a hospital, machinery, plumbing) that is built, constructed, installed, or established to perform some particular function or to serve or facilitate some particular end").

[19] The Department of Justice has further expanded upon the definition of "facility" to include "identifiers," such as "a specific cellular telephone identified by its electronic serial number; an Internet user account or e-mail address; or an Internet Protocol address, port number, or similar computer network address or range of addresses." Computer Crime and Intellectual Property Section, Department of Justice, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, at 4 (2001), https://perma.cc/QA8Z-5C9G; *see also* H.R. Rep. No. 107-236, at 52–53 (2001). Such identifiers function in much the same way as a traditional telephone number, identifying the logical endpoint to which a

does not include the end-user devices that transmit or receive that communication. *Cf.* Computer Crime and Intellectual Property Section, Department of Justice, *Prosecuting Computer Crimes* 90–91 (2d ed. 2010) (distinguishing between an end-user device and a "facility through which an electronic communication service was provided").

Statutory context confirms that a "facility" to which a pen-trap device can be attached or applied does not include end-user devices. Most immediately, § 3123 identifies the "packet-switched data network of" an electronic service provider as one example of a type of facility to which a pen-trap device could be attached or applied. 18 U.S.C. § 3123(a)(3)(A). "A packet-switched network transports data units called packets through a maze of switches where packets are queued and routed towards their destination. . . . A packet-switched network has a network core consisting of routers and control systems interconnected by very-high-bandwidth communication channels and a network edge where the end-user systems reside." Marinescu at 176 (emphases omitted). Such networks are internet service providers' equivalent of the circuit-switched networks utilized by telephone companies at the time of ECPA's enactment. *See* Bellovin et al., 30 Harv. J.L. & Tech. at 37. That is, a packet-switched network serves the same function as a telephone line—it is the infrastructure that facilitates the transmission of an electronic communication from one end-user device to other end-user devices.

The enacted definitions of "pen register" and "trap and trace device" also support this conclusion. A pen register "records or decodes" DRAS information "*transmitted* by an instrument or facility from which a wire or electronic communication is *transmitted*"—*i.e.*, an end-user device. 18 U.S.C. § 3127(3) (emphases added). The drafters' use of the past tense "transmitted" indicates that the communication must have already

---

communication should be directed. *See* DOJ, *Searching & Seizing* at 229–30. Although it is perhaps counterintuitive to call an identifier a "facility," *see* 18 U.S.C. § 3123(b)(1)(C) (distinguishing between the "number or other identifier" and the "location of the telephone line or other facility to which the [pen-trap device] is to be attached or applied"), courts have largely concurred with this interpretation, *see In re Application of the U.S. for PRTT Order for One WhatsApp Chief Acct. for Investigation of Violation of 21 U.S.C. § 841*, No. 18-pr-17, 2018 WL 1358812, at *4 (D.D.C. Mar. 2, 2018) (collecting cases). What is clear, however, is that neither the Department of Justice nor the courts have historically interpreted "facility" in this context as including an end-user device itself.

been sent from the originating end-user device at the time that the pen register "record[s] or decode[s]" the DRAS information. Goldfoot, 6 Va. J. Crim. L. at 36–37. A trap-and-trace device "captures the *incoming* electronic or other impulses which identify the originating number or other" DRAS information. 18 U.S.C. § 3127(4) (emphasis added). That the "electronic or other impulses" are "incoming" at the time they are "capture[d]," *id.*, reveals that they have not been acquired by the receiving end-user device, *see* Goldfoot, 6 Va. J. Crim. L. at 37–38. The combined definitions of pen register and trap-and-trace device therefore demonstrate that a pen-trap device must act on a communication traveling between end-user devices, not on the end-user devices themselves. The definition of a "facility" on which a pen-trap device can be installed must be circumscribed accordingly.

c.

The Pen-Trap Statute also distinguishes a "facility" on which a pen-trap device can be installed from the "electronic or other impulses" on which the communication is encoded. 18 U.S.C. § 3127(4).

Start with the basics of telecommunication. Every transmitting end-user device must first convert its communication into "electronic or other impulses." *Id.*; *see also* ScienceInsights, *How Telecommunication Works: From Signals to 5G* (Mar. 4, 2026), https://perma.cc/U7AC-DJLF ("ScienceInsights"). That device then transmits the impulses to the receiving end-user device via a communication channel. *See* ScienceInsights. Some communication channels, such as traditional landline telephones, rely entirely on intermediary infrastructure—the electronic pulses leave the transmitting telephone and travel along a copper wire until they reach the receiving phone. Other channels involve no such intermediary infrastructure. For example, the ground control station of a typical UAS utilizing line-of-sight radiofrequency communications converts its communications into radio waves ("other impulses") and transmits them through the air directly to the unmanned aircraft. Still others, such as cellular communications, partially rely on intermediary infrastructure. A transmitting cell phone, for instance, converts a voice message into radio waves and transmits them to a cell tower, which further converts those radio waves into light or electronic impulses that travel along cellular network infrastructure to another cell tower, where the communication is converted back into radio waves for interception by the receiving cell

phone. A facility that facilitates the transmission of a communication does so by facilitating the transmission of the impulses on which the communication is embedded. Because the plain meaning of "facility" does not include that which it facilitates, the meaning of the term "facility," for the purposes of the Pen-Trap Statute, does not include the impulses that the facility conveys.

Other statutory clues further underscore this conclusion. A pen-trap device is "attached or applied" to a "telephone line or other facility." 18 U.S.C. § 3123(b)(1)(A), (C). But the device "records," "decodes," or "captures" the impulses that are transmitted by an end-user device and conveyed by the facility to which the device is attached or applied. *Id.* § 3127(3), (4). The Pen-Trap Statute thus distinguishes between a "facility" and the "electronic or other impulses" that the facility conveys or relays.

Describing "electronic or other impulses" as a "facility" would also render § 3123 nonsensical. Impulses are not "leased" or "own[ed]," nor can they otherwise be "listed" in a person's name. *Id.* § 3123(b)(1)(A), (d)(2). Similarly, it would be nearly impossible to identify the "location of" an impulse, *id.* § 3123(b)(1)(C), or require a communication service provider, landlord, custodian, or other person to "install" a pen-trap device on the "appropriate" impulse, *id.* § 3124(b). And the necessary court order itself would have to require multiple "installations" under that interpretation, because a communication is often transmitted by a series of impulses; to "record," "decode," or "capture" a single impulse would provide the government with virtually no DRAS information, thereby undermining the statute's purpose of facilitating such collection.

An "electronic or other impulse" is therefore not a "facility" on which a pen-trap device can be installed.

* * *

In summary, the words "use" and "facility," and the definitions of pen registers and trap-and-trace devices, are potentially broad, but their breadth for purposes of the Pen-Trap Statute is circumscribed by statutory context and logical structure. That structure indicates that a prerequisite to the "use" of a pen-trap device is that the device be "installed." The only place such a device can be "installed" is on a "telephone line or other facility." And such a "facility" does not include either the end-user device or the "electronic or other impulses" that the facility conveys

or relays. Even if a device would otherwise fall within the definitions of "pen-register" or "trap and trace device," then, its "use" would violate the statute only if that device was first attached or applied to a telephone line or other facility.

3.

We have considered four counterarguments to our interpretation, but none persuades.

a.

It could be argued that we have given insufficient weight to the disjunctive "or" separating "install *or* use" in § 3121(a) (emphasis added), such that our interpretation fails to give full effect to the Pen-Trap Statute's "expansive prohibition." Goldfoot, 6 Va. J. Crim. L. at 5. To be sure, the statute prohibits each act independently of the other. But our interpretation is entirely consistent with separate prohibitions. That is, one could violate the statute by installing a pen register or a trap-and-trace device without using it. And one could violate the statute by using a device that someone *else* installed. But one cannot be convicted for using a device or process that was never "installed" in the first instance. The fact that Congress desired to criminalize both the installation and use of a pen-trap device says little about whether its "installation" is a logical prerequisite to its "use."

A related argument is that our interpretation impliedly adds elements to the Pen-Trap Statute's criminal prohibition. Specifically, for a person to be convicted of "using" a pen-trap device, a prosecutor would also have to prove that the device used was "installed" on a "telephone line or other facility." This arguably violates the maxim that "words or elements" should not be read "into a statute." *Dean v. United States*, 556 U.S. 568, 572 (2009); *see also Application of Section 191*, 50 Op. O.L.C. at *9 ("It is a bedrock principle of statutory construction that 'nothing is to be added to what the text states or reasonably implies.'" (alteration adopted) (quoting Scalia & Garner at 93)).

But textual interpretation involves more than simply reading words in isolation. "The plainness or ambiguity of statutory language is determined by reference to the language itself, the specific context in which the language is used, and the broader context of the statute as a whole." *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997). Indeed, "no

interpretive fault is more common than the failure to follow the whole-text canon, which calls on the . . . interpreter to consider the entire text, in view of its structure and of the physical and logical relation of its many parts." Scalia & Garner at 167. Our reading does not add elements to the Pen-Trap Statute's prohibition but instead makes explicit what the statutory context reasonably implies. As we have established, the conjunctive pairing of "install" and "use" throughout the statute demonstrates that a pen-trap device must be "installed" before it can be "used." *See supra* Part II.A.2.a. The canon of consistent usage thus suggests that "use" in § 3121(a) should likewise bear this narrower meaning.

True, unlike the remainder of the statute, "install" and "use" in § 3121(a) are disjunctive. *See* 18 U.S.C. § 3121(a). But untethering "use" from the requirement that a pen-trap device first be installed would result in "improbable consequences." *Fischer*, 603 U.S. at 488. It could categorically prohibit the use of any device that cannot first be installed—after all, the government may only seek, and a court may only grant, an order "authorizing the *installation and use* of a" pen-trap device. 18 U.S.C. § 3123(a)(1) (emphasis added); *see also id.* § 3122(a). Such a result would be particularly anomalous given that in enacting the Pen-Trap Statute, Congress sought to create a technologically neutral mechanism by which the government could obtain DRAS information. *See* Bellovin et al., 30 Harv. J.L. & Tech. at 16–17; Kerr, 97 Nw. U. L. Rev. at 637–38. Given these considerations, it is best to resolve the potential ambiguity in favor of narrower criminal liability and greater internal consistency.

Our conclusion that a pen-trap device must be installed "on a telephone line or other facility" before it can be used similarly does not add an element to the Pen-Trap Statute's prohibition; it simply clarifies the meaning of "install" and "use." It would make little sense to convict someone for "installing" a pen-trap device on an object that renders the pen-trap device obviously ineffective. *See Fischer*, 603 U.S. at 488. For example, a pen register of old could record or decode numbers dialed by a telephone if clipped to a telephone line, but if it was clipped to a door-frame, it would be completely useless. A modern device might be capable of capturing the light pulses traversing a fiberoptic cable, but if it is "installed" on a desk instead of a fiberoptic line, it too would be useless. The surrounding statutory provisions make clear that Congress sought to criminalize the installation of pen-trap devices on telephone lines and other physical or digital infrastructure that facilitate the transmission of

wire or electronic communications, *see supra* Part II.A.2.b, as only installation on such objects renders a pen-trap device useable, *see* 18 U.S.C. § 3127(3)–(4).[20]

Unmooring "installation" and "use" from the Pen-Trap Statute's context would introduce other inconsistencies into federal law, too. Just as statutory words and phrases must be construed in the light of their surrounding text, so too must "[w]e construe federal laws harmoniously to effectuate Congress's enactments to the extent possible, particularly when statutes address the same subject." *Harmonizing the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 and Section 214 of the Housing and Community Development Act of 1980*, 50 Op. O.L.C. __, at *7 (Feb. 18, 2026). ECPA contains provisions regulating the acquisition of both DRAS information (the Pen-Trap Statute) and communicative contents (the Wiretap Act amendments). But an interpretation of the Pen-Trap Statute that does not require a pen-trap device to first be installed on a telephone line or other facility before that device can be "used" would fit uneasily with ECPA's Wiretap Act exceptions.

For instance, the Wiretap Act permits the government to intercept an electronic communication where a person who "is a party to the communication . . . has given prior consent to such interception." 18 U.S.C. § 2511(2)(c). The victim of an online financial fraud scheme might authorize the government to intercept his email correspondence with the fraudster by installing certain firmware on his personal computer's network-interface card. Capturing the content of the emails would be lawful under the Wiretap Act because "a party to the communication" gave "prior consent to such interception." *Id.* But capturing the metadata associated with the email correspondence would run afoul of an unmoored interpretation of the Pen-Trap Statute—the firmware used to intercept the emails would constitute an unlawful pen-trap device. *See id.* § 3127(3)–(4); *see also* Mysti Degani & Louisa Marion, *Making the Most of Your Statutory Electronic Evidence Toolbox*, U.S. Att'ys' Bull., May 2016, at 56, 60. Such an interpretation would thus bizarrely prohibit collecting the DRAS information, even though the Wiretap Act allows the government to intercept the emails' content. *See* Ohm, 2009 U. Ill. L. Rev. at 1480 (observing this anomaly); Kerr, 97 Nw. U. L. Rev. at

[20] Installation on an end-user device could also render the pen-trap device effective. But the word "facility" must exclude end-user devices for the reasons provided above in Part II.A.2.b.

630–31 (noting that Congress has provided strong protections for the interception of content and provided "little if any protection" for DRAS information); *cf. United States v. Freeman*, 524 F.2d 337, 341 (7th Cir. 1975) (rejecting a similar "anomalous, if not absurd, result" that would have prohibited "a lesser intrusion of privacy" while allowing "a greater intrusion" under the Wiretap Act). Our interpretation, by contrast, harmonizes these provisions. Even though the firmware might fall within the Pen-Trap Statute's definitions of "pen register" and "trap and trace device," it is not installed on a "telephone line or other facility"; it is instead installed on an end-user device. The government agent would therefore not be "us[ing]" a pen-trap device within the meaning of the Pen-Trap Statute's prohibition. 18 U.S.C. § 3121(a).

Unmooring "use" from "install" would also criminalize "everyday conduct." Goldfoot, 6 Va. J. Crim. L. at 4; *see also Fischer*, 603 U.S. at 497 (disfavoring such an expansive result and "exercis[ing] restraint in assessing the reach of a federal criminal statute"). Our interpretation, by contrast, averts such anomalies. For instance, our interpretation avoids criminalizing normal processes that are required for the internet to function. *See* Goldfoot, 6 Va. J. Crim. L. at 15–16. To see why, consider standard internet communication protocols: Computer A transmits data packets through internet service providers to Computer B. *See* Kerr, 97 Nw. U. L. Rev. at 613–14. Computer B receives not only the communicative contents but also the addressing information for those data packets—such as Computer A's IP address and other non-content routing information. *See id.* at 614; *see also* Kerr, *Computer Crime Law* at 627 (explaining that the Pen-Trap Statute "clearly includes IP addresses"). If a pen register or a trap-and-trace device could be used without first having been installed on a telephone wire or other facility, then Computer B would operate as an illegal trap-and-trace device in its receipt of those data packets; indeed, the receipt of practically any internet communication would be illegal. *See* Goldfoot, 6 Va. J. Crim. L. at 15–16. But under our interpretation, Computer B would not violate the statute because the software used to capture the addressing information is installed on an end-user device (Computer B), not on a telephone line or other facility.[21]

[21] Under either a broad or narrow interpretation, the software used by internet service providers to capture the DRAS information is exempt from the Pen-Trap Statute's prohibition, as it "relat[es] to the operation" of the internet service providers' "electronic communication service." 18 U.S.C. § 3121(b)(1).

Or consider cell phones, which maintain call logs that list "[phone] numbers that the phone's user has called or attempted to call." *Id.* at 14. Such software could be considered a pen register because it records dialing information transmitted by the phone, which is "an instrument . . . from which a[n] . . . electronic communication is transmitted." 18 U.S.C. § 3127(3). Under a broad reading, both the cell-phone manufacturer (which installed the software) and the cell-phone user (who uses the software) would violate the Pen-Trap Statute. *See* Goldfoot, 6 Va. J. Crim. L. at 14. But under our reading, neither party violates the statute, because the software was never attached or applied to a telephone line or other facility; it exists only on the end-user device (the cell phone).

At bottom, statutory interpretation is an exercise in giving effect to the law that Congress passed as Congress passed it—not to "make a hash" of the language and render it unworkable. *Becerra v. Empire Health Found., for Valley Hosp. Med. Ctr.*, 597 U.S. 424, 438 (2022); *see also Cedar Rapids Cmty. Sch. Dist. v. Charlene F. ex rel. Garret F.*, 526 U.S. 66, 73–76 (1999). Faced with a choice between two plausible interpretations of the Pen-Trap Statute, choosing the interpretation that would not yield absurd results is "perfectly valid." Scalia & Garner at 237; *cf. Pulsifer*, 601 U.S. at 152–53. Congress evidently did not mean to ban the internet in a PATRIOT Act amendment designed to permit government surveillance of, and arguably protect, the internet. *See* Bellovin et al., 30 Harv. J.L. & Tech. at 16–17; Kerr, 97 Nw. U. L. Rev. at 637–38. And "[a]lthough a statute's purpose can never overcome the statutory text, 'a textually permissible interpretation that furthers rather than obstructs the document's purpose should be favored.'" *Application of Section 191*, 50 Op. O.L.C. at *16 (alteration adopted) (quoting Scalia & Garner at 63).

b.

Another counterargument is that "facility" is used throughout the Pen-Trap Statute in multiple different contexts.[22] The definition of "facility" should therefore not be circumscribed by "telephone line" but should

[22] *See, e.g.*, 18 U.S.C. §§ 3124(a) ("information, facilities, and technical assistance necessary to accomplish the installation of the pen register"), 3126(4) ("the number and nature of facilities affected"), 3127(3) (DRAS "transmitted by an instrument or facility from which a wire or electronic communication is transmitted").

instead be given a breadth that permits it to be used consistently in whatever context it appears.

Though we typically presume that "identical words used in different parts of the same act are intended to have the same meaning," *Application of Record Destruction Requirements to Information Received from the National Instant Criminal Background Check System*, 29 Op. O.L.C. 17, 22 (2005) (quoting *Comm'r v. Lundy*, 516 U.S. 235, 250 (1996)), that presumption "'readily yields' to context, and a statutory term . . . 'may take on distinct characters from association with distinct statutory objects calling for different implementation strategies,'" *Util. Air Regul. Grp. v. EPA*, 573 U.S. 302, 320 (2014) (quoting *Env't Def. v. Duke Energy Corp.*, 549 U.S. 561, 574 (2007)). Such is the case here.

As noted, the word "facility" means "something designed, built, installed, etc., to serve a specific function affording a convenience or service." *Random House 2001* at 690.[23] That definition is broad enough to include everything from an end-user device to intermediary communication infrastructure, a landlord's utilities closet, and a nuclear-missile silo. *See In re [Redacted] Non-U.S. Persons*, No. 19-218, at 7 n.5 (FISA Ct. Mar. 5, 2019) (observing that "'facilities' means practically anything you want it to mean so long as it covers a sufficiently broad variety of 'things' which you haven't got a convenient name for" (quoting *Newton's Telecom Dictionary* 518 (30th ed. 2016))); 10 U.S.C. § 130i(m)(4)(A) (using the term "facility" to include objects and locations pertaining to "nuclear deterrence" and "missile defense").

Such breadth requires that "facility" be circumscribed by the context in which it appears. *See Jarecki*, 367 U.S. at 307; *see also Yates*, 574 U.S. at 543 (plurality opinion). For instance, § 3127(3)'s context reveals that "facility" denotes the end-user device from which a communication originates. That is because the "facility" at issue must have the ability to transmit (*i.e.*, originate) "a wire or electronic communication." 18 U.S.C. § 3127(3). The statute's pairing of "facility" with "instrument" confirms this result. An "instrument" is "a mechanical tool or implement," *Random House 2001* at 988,[24] that, like a facility, must have the

[23] *See also Webster's Third 2002* at 812–13 (defining "facility" as "something (as a hospital, machinery, plumbing) that is built, constructed, installed, or established to perform some particular function or to serve or facilitate some particular end").

[24] *See also Webster's Third 2002* at 1172 (defining "instrument" as "a means whereby something is achieved, performed, or furthered," or a "utensil, implement").

ability to originate a wire or electronic communication, *see* 18 U.S.C. § 3127(3). Indeed, the quintessential example of such an "instrument" is a telephone set. *See* Goldfoot, 6 Va. J. Crim. L. at 37 ("Congress presumably meant the word 'instrument' to have the same meaning as in the Wiretap Act, where it refers to physical telephone equipment . . . ."); *see also* 18 U.S.C. § 2510(5)(a) (describing "telephone or telegraph instrument[s]").

By contrast, the use of "facility" in describing what a "landlord, custodian, or other person" must furnish to law enforcement pursuant to a pen-trap order is quite broad. 18 U.S.C. § 3124(a)–(b). It includes, for example, entrance into a landlord's utility closet where a router or telephone junction box is located, access to a communication service provider's packet-switched data network, or anything else "necessary to accomplish the installation of the" pen-trap device, *id.* § 3124(a). Yet "facility" here cannot include end-user devices. Such devices (and the premises on which they are found) are protected from governmental access by the Fourth Amendment's warrant requirement. *See Riley*, 573 U.S. at 403 (holding that law enforcement must obtain a warrant before searching a cell phone); *Chapman v. United States*, 365 U.S. 610, 610–12, 617–18 (1961) (holding that a landlord's consent does not necessarily alleviate law enforcement's responsibility to obtain a warrant before entering an apartment). A pen-trap order, with its minimal "relevancy" requirement, *see* 18 U.S.C. § 3122(b)(2), therefore cannot command a "landlord, custodian, or other person" to provide access to such a "facility," *id.* § 3124(a)–(b).

These two examples demonstrate the statute's flexible use of the word "facility." In § 3127, "facility" *only* includes originating end-user devices, while in § 3124, "facility" entirely *excludes* end-user devices while embracing significantly more physical and digital infrastructure. It is therefore unsurprising that "facility" as used in § 3123(b)—where it is paired with a different object (*i.e.*, "telephone line") and a different phrase (*i.e.*, "to which the pen register or trap and trace device is to be attached or applied")—bears a different meaning.

Our interpretation also accounts for "the basic logic that Congress would not go to the trouble of" pairing "facility" with different words and phrases if "facility" merely swallowed up those words. *Fischer*, 603 U.S. at 489–90. Congress in the PATRIOT Act intentionally paired "facility" with "telephone line" throughout that statute's text, PATRIOT

Act § 216(b)(2)–(3), (c)(6), 115 Stat. at 289–90, yet in one instance paired "facility" with "instrument," *id.* § 216(c)(2), 115 Stat. at 290. Without context, the word "facility" can be broad enough to subsume both "telephone line" and "instrument." The best way to give these terms meaning, and the most sensible inference available here, is to limit the scope of "facility" based on Congress's intentional pairing. *See Fischer*, 603 U.S. at 486–90.

c.

Some might say that our interpretation does not sufficiently account for the Pen-Trap Statute's privacy rationale. But characterizing the Pen-Trap Statute as a privacy statute is only part of the story. True, it is contained within the "Electronic Communications *Privacy* Act," ECPA § 1, 100 Stat. at 1848 (emphasis added), and that title is admittedly a "permissible indicator[] of meaning," Scalia & Garner at 221. But as it relates to the government's ability to obtain information, the statute is best understood as codifying federal judicial authority to issue orders directed at communication service providers. As already noted, the information obtained by pen-trap devices is *not* constitutionally protected. *See Smith*, 442 U.S. at 745–46; *supra* Part II.A.1. Yet when the government sought this information from communication service providers, some resisted the makeshift orders issued by inferior courts. *See* Goldfoot, 6 Va. J. Crim. L. at 11. Far from providing a stronger shield of subscriber privacy, Congress provided that courts "shall enter" such orders, 18 U.S.C. § 3123(a)(1), so long as an application certifies "that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by [the submitting] agency," *id.* § 3122(b)(2). One need not look far to see that Congress set a lower privacy threshold for DRAS information here than it did for similar subscriber information in other statutory contexts.[25]

[25] For example, to obtain under the Stored Communications Act "a record or other information pertaining to a subscriber to or customer of [an electronic communications] service (not including the contents of communications)," the government must offer "*specific and articulable facts* showing that there are *reasonable grounds* to believe that the contents of a wire or electronic communication, or the records or other information sought, are *relevant and material* to an ongoing criminal investigation." 18 U.S.C. § 2703(c)(1), (d) (emphases added). Similarly, the Right to Financial Privacy Act requires the government to have "reason to believe that the records sought are relevant to

Insofar as the Pen-Trap Statute protects privacy, our interpretation retains the statute's core prohibitions. Whenever the government seeks DRAS information by way of a telephone line or other facility, it must still seek a court order under the Pen-Trap Statute. Nongovernmental actors likewise remain prohibited from installing or using pen-trap devices on telephone lines and other facilities. Where DRAS information can be acquired without attaching or applying a pen-trap device to a telephone line or other facility, the Fourth Amendment protects those transmissions from government intrusion to the extent that the sender or recipient has a reasonable expectation of privacy in the information. *See Chatrie*, 609 U.S. at 619–20; *Carpenter*, 585 U.S. at 304–05. And the Wiretap Act continues to prohibit the government and citizens alike from unlawfully intercepting communicative contents. 18 U.S.C. § 2511(1).

d.

Finally, an argument could be made that our interpretation renders portions of the statutory C-UAS authorities superfluous. Each statutory authority relieves officials from criminal liability under a variety of preexisting federal laws, including the Pen-Trap Statute. *See* 6 U.S.C. § 124n(a); 10 U.S.C. § 130i(a); *id.* § 6227(a); 50 U.S.C. § 3515a(a). Yet the UAS-detection technologies that we have assessed are not attached or applied to a "telephone line or other facility," so it might be argued that statutory relief from the Pen-Trap Statute was unnecessary.

But this argument overlooks Congress's effort to create a durable statute in the face of technological change. True, the technologies that you have asked us to consider do not ultimately violate the Pen-Trap Statute because they do not typically operate on a "telephone line or other facility." *See infra* Part III. But the rapid development of UAS technology may require C-UAS technology to do so in the future. *See* Maresch at 326; *see also* Brungardt & Carraway at 64. For instance, 5G wireless broadband mobile-communication networks may be used to conduct

---

a legitimate law enforcement inquiry," and to serve a copy of the subpoena along with a specified notice on the customer. 12 U.S.C. § 3405. That Act then grants the customer standing to challenge the subpoena. *See id.* § 3410. Like information obtained by pen-trap devices, neither subscriber information nor bank records are protected by the Fourth Amendment. *See United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (involving subscriber information and collecting cases); *United States v. Miller*, 425 U.S. 435, 440–43 (1976) (involving bank records).

beyond-line-of-sight UAS operations. *See* Brungardt & Carraway at 64. The government's use of a C-UAS system attached or applied to a wireless provider's network infrastructure for the purpose of recording, decoding, or capturing a UAS's DRAS information traveling on that network would likely violate the Pen-Trap Statute without statutory relief. Simply because UAS-detection technology does not currently require statutory relief from the Pen-Trap Statute's prohibition does not mean that it never will require such relief.

Another reason for Congress's inclusion of the Pen-Trap Statute among the statutory reliefs may have been the statute's historically uncertain coverage and the absence of judicial precedent interpreting it. Its inclusion among the reliefs thus provides additional assurance that criminal liability will not attach to UAS detection performed under the statutory authorities. Such statutory provisions, although "technically unnecessary," may nevertheless be "inserted out of an abundance of caution." *Fort Stewart Schs. v. Fed. Lab. Rels. Auth.*, 495 U.S. 641, 646 (1990); *see also Smith v. City of Jackson*, 544 U.S. 228, 252 (2005) (O'Connor, J., concurring in the judgment) ("[C]odifying an express statutory exemption from liability" may "merely demonstrate[] Congress' abundance of caution." (emphasis omitted)).

* * *

We conclude that to "use" a pen-trap device in violation of the Pen-Trap Statute, that device must first be "attached or applied" to a "telephone line or other facility." The word "facility" does not include an end-user device or the "electronic or other impulses" used to convey a communication between end-user devices.

B.

ECPA also amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, commonly known as the "Wiretap Act," to govern the interception of wireless communications. ECPA §§ 101–111, 100 Stat. at 1848–59.

Congress originally enacted the Wiretap Act in response to the Supreme Court's Fourth Amendment decisions in *Berger v. New York*, 388 U.S. 41 (1967), and *Katz v. United States*, 389 U.S. 347 (1967). *See Wiretapping and Eavesdropping* § 1:7. The Wiretap Act, as amended,

prohibits any person, including law enforcement, from "intentionally intercept[ing]" or "endeavor[ing] to intercept . . . any wire, oral, or *electronic communication*." 18 U.S.C. § 2511(1)(a) (emphasis added). Subject to certain exclusions not relevant here, the term "'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." *Id.* § 2510(12).[26] "'[I]ntercept' means the aural or other acquisition of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4) (emphasis added). And "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).[27]

Of the UAS-detection technology you have asked us to assess, only radiofrequency-detection systems that identify UAS remote-identification broadcasts or extract data directly from a communications link intercept a communication's content for purposes of the Wiretap Act. That is because UAS remote-identification broadcasts and information sent via UAS communications links are electronic communications, *see supra* Part I.A–B, and radiofrequency-detection systems that identify such broadcasts or extract such information acquire the contents of those communications. Section 2511(2)(g)(i), however, permits any individual to

[26] The electronic communication must also "affect interstate or foreign commerce." 18 U.S.C. § 2510(12). We assume for purposes of this opinion that the UAS communications subject to detection or interception in any particular case satisfy this requirement.

[27] As a general matter, DRAS information includes the data required to establish, maintain, route, and direct communications between the ground control station and the unmanned aircraft. *See* DOJ, *Searching and Seizing* at 154 (maintaining that "'dialing, routing, addressing, and/or signaling information' encompasses almost all non-content information in a communication" (alteration adopted)); *see also* 18 U.S.C. § 3121(c) (describing DRAS information as "utilized in the processing and transmitting of wire or electronic communications"). Examples include IP addresses, port numbers, session-identification numbers, MAC addresses, and related messages required to set up, maintain, and tear down the communication links. Content, by contrast, includes the substance of all messages sent between the unmanned aircraft to the ground control station, such as the unmanned aircraft's location, speed, heading, battery status, video and sensor data, and command inputs. *See* 18 U.S.C. § 2510(8); Kerr, 97 Nw. U. L. Rev. at 645–46.

"intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is *readily accessible to the general public*." 18 U.S.C. § 2511(2)(g)(i) (emphasis added).[28]

To interpret this Wiretap Act exception, we first analyze whether UAS communications fall within the subset of electronic communications known as "radio communication[s]," for which there is a statutory definition to determine whether such communications are "readily accessible to the general public." *Id.* § 2510(16). Though we conclude that UAS communications could be construed as "radio communications," we note that some courts will hold that they are non-radio "electronic communications," for which there is no statutory definition of "readily accessible to the general public." To determine whether a non-radio electronic communication is "readily accessible to the general public," we therefore go on to define that phrase based on its ordinary meaning.

1.

The Wiretap Act allows interception of an "electronic communication" under § 2511(2)(g)(i) only if such communication is "made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public."[29] "Radio communication[s]" are a subset of electronic communications. *See id.* § 2510(12). And a "radio communication" is "readily accessible to the general public" unless it is

> (A) scrambled or encrypted;
>
> (B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

[28] Other potentially applicable Wiretap Act exceptions may exist with respect to radiofrequency detection generally and remote-identification broadcasts specifically. *See, e.g.*, 18 U.S.C. § 2511(2)(c), (d), (g)(ii)(I), (II), (IV). But because we determine that remote-identification broadcasts fall within § 2511(2)(g)(i)'s exception, we do not further consider those other exceptions here.

[29] A separate Wiretap Act exception exists for "any *radio communication* which is transmitted . . . by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, *readily accessible to the general public*." 18 U.S.C. § 2511(2)(g)(ii)(II) (emphases added).

> (C) carried on a subcarrier or other signal subsidiary to a radio transmission;
>
> (D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
>
> (E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission,[30] unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.

18 U.S.C. § 2510(16); *see also Wiretapping and Eavesdropping* § 2:144; S. Rep. No. 99-541, at 14 (1986).

The Wiretap Act does not define "radio communication." That phrase could bear a technical meaning that encompasses any information transmitted using radio waves—*i.e.*, any communication over the radio-frequency band of the electromagnetic spectrum. *See* 13 *Oxford English Dictionary* 95 (2d ed. 1989) ("*Oxford Second*") (defining "radio" as "[t]he transmission and reception of radio-frequency electromagnetic waves, esp[ecially] as a means of communication that does not need a connecting wire").[31] If so applied, UAS communications, including remote-identification broadcasts, would be "radio communication[s]" because

---

[30] *See* 47 C.F.R. §§ 25.101–25.109 ("Satellite Communications"); *id.* §§ 74.401–74.482 ("Remote Pickup Broadcast Stations"); *id.* §§ 74.501–74.582 ("Aural Broadcast Auxiliary Stations); *id.* §§ 74.600–74.690 ("Television Broadcast Auxiliary Stations").

[31] *See also Webster's Third 1993* at 1872 (defining "radio" as "the transmission and reception of electric impulses or signals by means of electromagnetic waves without a connecting wire [(]includes wireless, television, and radar[)]"); *Random House 1987* at 1592 ("wireless telegraphy or telephony"); *Webster's Ninth New Collegiate Dictionary* 971 (1985 ed.) ("the wireless transmission and reception of electric impulses or signals by means of electromagnetic waves"); *Webster's New World Dictionary* 1107 (3d coll. ed. 1988) ("the practice or science of communicating over a distance by converting sounds or signals into electromagnetic waves and transmitting these directly through space, without connecting wires, to a receiving set, which changes them back into sounds, signals, etc."); *Webster's II New Riverside University Dictionary* 969 (1988 ed.) ("[u]se of electromagnetic waves in the radio frequency range to transmit or receive electric signals without wires connecting the points of transmission and reception").

they are transmissions of information by radio wave. *See* 18 U.S.C. § 2510(12). A UAS communication could therefore be intercepted under § 2511(2)(g)(i) so long as it does not fall within one of the categories deemed not "readily accessible to the general public" by § 2510(16).

But the Ninth Circuit has "conclude[d] that 'radio communication' should carry its ordinary meaning: a predominantly auditory broadcast." *Joffe v. Google, Inc.*, 729 F.3d 1262, 1270 (9th Cir. 2013) ("*Joffe I*"), *amended by* 746 F.3d 920 (9th Cir. 2013) ("*Joffe II*"). If a court applied this definition—as any court in the Ninth Circuit would—then UAS communications would *not* be "radio communications," because transmissions via UAS communications links are not predominantly auditory. In the Ninth Circuit, then, UAS communications would instead be considered a non-radio electronic communication for purposes of § 2511(2)(g)(i). And unlike with "radio communication," the Wiretap Act does not expressly dictate which non-radio electronic communications are readily accessible to the general public.

We must therefore determine what non-radio electronic communications fall within § 2511(2)(g)(i)'s exception. But we need not decide which definition of "radio communication" is ultimately correct because, as discussed below in Part III, remote-identification broadcasts fall within § 2511(2)(g)(i)'s exception under either approach. And under either approach, other UAS transmissions must be assessed on a case-by-case basis.

2.

To determine the meaning of "readily accessible to the general public" in § 2511(2)(g)(i), we begin with the text, *see Bufkin v. Collins*, 604 U.S. 369, 379 (2025), and "assum[e] that the ordinary meaning of that language accurately expresses the legislative purpose," *Expenditure of Appropriated Funds for Informational Video News Releases*, 28 Op. O.L.C. 109, 119 (2004) (quoting *Engine Mfrs. Ass'n v. S. Coast Air Quality Mgmt. Dist.*, 541 U.S. 246, 252 (2004)). "[U]nless otherwise defined, statutory terms are generally interpreted in accordance with their ordinary meaning." *Sebelius v. Cloer*, 569 U.S. 369, 376 (2013); *see also Fed. Deposit Ins. Corp. v. Meyer*, 510 U.S. 471, 476 (1994). Here, the phrase "readily accessible to the general public" is only defined with respect to "radio communication," 18 U.S.C. § 2510(16), so we rely on

that phrase's ordinary meaning to ascertain its scope in the context of non-radio "electronic communications."

The Wiretap Act reads: "It shall not be unlawful under this chapter . . . to intercept or access an *electronic communication* made through an *electronic communication system* that is *configured* so that such electronic communication is *readily accessible* to the *general public*." 18 U.S.C. § 2511(2)(g)(i) (emphases added). The independent clause ("It shall not be unlawful under this chapter . . . to intercept or access an electronic communication") makes clear that individuals may intercept or access certain electronic communications. *Id.* The remaining portion of the sentence identifies what types of electronic communications one may intercept.

Electronic communications subject to interception must be made through an electronic communication system—that is, "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.* § 2510(14). But not just any electronic communication system: It must be a system identified by the relative clause ("that is configured. . . ."). *Id.* § 2511(2)(g)(i). "Configured" acts as a participial adjective describing the state of the electronic communication system. The "electronic communication system" must therefore, as an objective matter, incorporate "elements" that permit it "to perform a certain task or provide a certain capability." 3 *Oxford Second 1989* at 708.[32]

That "task" or "capability" is defined in the results clause: "so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). "Readily accessible" serves as the subject complement to "electronic communication." That is, it describes a necessary characteristic of the "electronic communication." *See id.* The ordinary meaning of "readily" is "promptly; quickly; easily." *Random House 1987* at 1606.[33] And the ordinary meaning of "accessible" is

[32] A similar participial adjective definition of "configured" can be derived from other contemporaneous dictionaries. *See, e.g.*, *Random House 1987* at 428; *Webster's Third 1993* at 476.

[33] *See also Webster's Third 1993* at 1889 (defining "readily" as "with a fair degree of ease : without much difficulty : with facility : easily"); 13 *Oxford Second 1989* at 264 (defining "readily" as "[p]romptly, in respect of the time of action; quickly, without delay; also, without difficulty, with ease or facility").

"obtainable; attainable." *Id.* at 11.[34] So the "electronic communication" at issue must be easily obtainable. The prepositional phrase within the results clause then specifies by whom the electronic communication must be easily obtained—the "general public." *See id.* at 795 (defining "general" as "not limited to one class, field, product, service, etc."); *id.* at 1562–63 (defining "public" as "the people constituting a community, state, or nation").[35]

Putting this all together, an individual may intercept or access electronic communications transmitted by an electronic communication system that incorporates elements which make the transmitted electronic communication easily obtainable by the general public. This analysis turns on the objective characteristics of the electronic communication system, not the subjective expectations of its user. The incorporation of any system element that attempts to prevent access is therefore sufficient to remove the system from § 2511(2)(g)(i)'s exception, even if those means are ineffective. But, as in the context of a related ECPA provision, "a person may reasonably conclude that a communication is readily accessible to the general public . . . if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy." *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1200 (9th Cir. 2022) (alterations adopted) (quoting H.R. Rep. No. 99-647, at 62 (1986)); *see also* Benjamin D. Kern, *Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law*, 21 Santa Clara Comput. & High Tech. L.J. 101, 130 (2004) (advocating for an express-prohibition test that would "prohibit[] access only if a network operator has indicated that access is prohibited . . . by enabling password protection or otherwise"); *cf.* 18 U.S.C. § 2510(16) (codifying an objective approach for the assessment of whether radio communications are "readily accessible").[36]

---

[34] *See also Webster's Third 1993* at 11 (defining "accessible" as "capable of being used, seen, known, or experienced"); 1 *Oxford Second 1989* at 73 (defining "accessible" as "[c]apable of being entered or reached; easy of access; such as one can go to, come into the presence of, reach, or lay hold of; get-at-able").

[35] *See also Webster's Third 1993* at 944 (defining "general" as "applicable or pertinent to the majority of individuals involved: characteristic of the majority"); *id.* at 1836 (defining "public" as "the people as a whole").

[36] An "objective" approach based on the system's configuration conforms with the Senate Committee on the Judiciary's understanding of § 2511(2)(g)(i). *See* S. Rep.

In *Joffe*, the Ninth Circuit initially interpreted the ordinary meaning of § 2511(2)(g)(i) differently, but it later withdrew that portion of its opinion to allow for further fact-finding in the district court. *See Joffe I*, 729 F.3d at 1277–79, *amended by Joffe II*, 746 F.3d 920.[37] After concluding that "radio communication" carried its ordinary meaning and thus excluded electronic communications transmitted over Wi-Fi, the Ninth Circuit analyzed whether such communications over unencrypted Wi-Fi were nonetheless "readily accessible to the general public" under the ordinary meaning of 18 U.S.C. § 2511(2)(g)(i). It held that they were not. *See Joffe I*, 729 F.3d at 1277–79. The court reasoned that "Wi-Fi transmissions are not 'readily' available because they are geographically limited and fail to travel far beyond the walls of the home or office where the access point is located." *Id.* And although the public had ready access to technology necessary for intercepting unencrypted communications, *id.* at 1278 n.8, the court concluded that "the general public lacks the expertise to intercept and decode payload data transmitted over a Wi-Fi network," *id.* at 1278.

The Ninth Circuit was right to withdraw its approach, as its conclusion suffered at least three major flaws. First, it unmoored "readily accessible to the general public" from its grammatical context. The question is not whether the communication *is* readily accessible. The question is whether the *electronic communication system*—in *Joffe I*'s case, unencrypted Wi-Fi—is *configured so that* its transmitted electronic communications are readily accessible. The Ninth Circuit's now-abandoned approach would have read this language out of the statute. *Cf. Fischer*, 603 U.S. at 492–96; *Pulsifer*, 601 U.S. at 141–44; Scalia & Garner at 174. Second, *Joffe I* would have adopted a murkier standard of accessibility based on the totality of the circumstances. When deciding between two possible interpretations of a statute that carries both criminal and civil penalties, as the Wiretap Act does, an interpreter should prefer a statutory construction that provides clearer notice. *See Snyder v. United*

No. 99-541, at 18 ("The term 'configure' is intended to establish an objective standard of design configuration for determining whether a system receives privacy protection.").

[37] Google argued in its petition for rehearing that the court had manifestly erred by resolving whether unencrypted Wi-Fi is an "electronic communication" that is "readily accessible to the general public" under 18 U.S.C. § 2511(2)(g)(i). *See* Google's Petition for Rehearing and Rehearing En Banc at 1–2, *Joffe II*, 746 F.3d 920 (No. 11-17483). Considering the case's posture as an interlocutory appeal from a motion to dismiss, the Ninth Circuit partially granted Google's motion and amended its opinion to omit that discussion.

States, 603 U.S. 1, 15 (2024) (declining an "interpretation of the statute [that] would create traps for unwary" defendants). Third, the *Joffe I* approach ultimately would have *decreased* protections for electronic communications as technology developed. Take the facts in *Joffe I*. In 2013, it may have been true that "intercepting and decoding payload data communicated on a Wi-Fi network require[d] sophisticated hardware and software." 729 F.3d at 1278. But that may not be true in 2050. *See In re Innovatio IP Ventures, LLC Pat. Litig.*, 886 F. Supp. 2d 888, 893 (N.D. Ill. 2012) (rejecting the conclusion that Wi-Fi communications are accessible only with sophisticated technology). Congress surely did not intend to create an arms race between publicly available technology and privacy protections. Under our objective approach, the security of one's electronic communications depends on the transmission system's *reasonable attempt* to protect those communications, not the *effectiveness* of such an attempt.

* * *

In sum, UAS communications, such as remote-identification broadcasts, could be construed as either "radio communications" or non-radio "electronic communications." If understood to be radio communications, they are subject to interception under § 2511(2)(g)(i) so long as they do not fall within the categories listed in § 2510(16). If they are understood to be non-radio "electronic communications"—as they would be in the Ninth Circuit—then they may be lawfully intercepted under § 2511(2)(g)(i) so long as they are transmitted by an electronic communication system that incorporates elements which make the communication's contents easily obtainable by the general public.

III.

Having established the relevant legal frameworks, we now apply them to the categories of UAS-detection systems you have asked us to review. We emphasize that our analysis depends on the facts as we understand them; our conclusions might be different if the detection technology at issue operates in ways that are materially different than we have described.[38]

[38] For the avoidance of doubt, federal and SLTT agencies need not invoke § 124n's authorities when observing a UAS by the naked eye, as the naked eye is neither a pen-

A.

Acoustic detection systems do not operate on the electromagnetic spectrum. They absorb mechanical sound waves produced by unmanned aircraft rotors. *See supra* Part I.C.1. These sound waves do not transmit any "dialing, routing, addressing, or signaling information." 18 U.S.C. § 3127(3)–(4). By definition, then, these systems are not pen-trap devices. They do not "record[]," "decode[]," or "capture[]" any "dialing, routing, addressing, [or] signaling information" associated with a communication. *Id.* Federal and SLTT authorities may therefore deploy such technology without violating the Pen-Trap Statute. Acoustic detection systems also do not implicate the Wiretap Act because they do not intentionally "intercept" any "wire, electronic, or oral communication.[39]" *Id.* § 2510(4). Such systems passively receive, identify, and interpret contentless mechanical sound waves. *See supra* Part I.C.1.[40]

B.

Passive EO/IR Systems. Passive EO/IR UAS-detection systems operate in the visible and infrared range of the electromagnetic spectrum. They therefore cannot record, decode, or capture UAS dialing, routing,

---

trap device, *see* 18 U.S.C. § 3127(3)–(4), nor an "electronic, mechanical, or other device," *id.* § 2510(5). Federal and SLTT agencies may therefore freely share information obtained from visual observations, as § 124n's restrictions on information sharing do not apply. *See* 6 U.S.C. § 124n(e).

[39] The Wiretap Act defines "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation." 18 U.S.C. § 2510(2).

[40] It is possible that an acoustic array could intercept the oral communications of passersby. But law-enforcement and military personnel who deploy such systems in their ordinary course do so to detect the harmonic structure of unmanned aircraft rotors, not to intercept oral communications. They therefore cannot be held liable under the Wiretap Act because the interception of an oral communication would not be "intentional[]." 18 U.S.C. § 2511(1); *see also United States v. Townsend*, 987 F.2d 927, 930 (2d Cir. 1993) (holding that a "defendant's act must have been the product of [their] conscious objective rather than the product of a mistake or an accident"); *In re HIPAA Subpoena*, 961 F.3d 59, 65 (1st Cir. 2020); *Wiretapping and Eavesdropping* § 3:3 ("Inadvertent interception does not violate § 2511(1) and therefore is not criminally or civilly actionable. Interceptions must be intentional to violate § 2511(1)" (footnote omitted)). Federal and SLTT law-enforcement agencies and military personnel employing acoustic technologies should minimize the risk of accidentally intercepting oral communications and configure their systems to discard any inadvertently intercepted oral communications.

addressing, or signaling information, which is transmitted via radio wave.[41] Using passive EO/IR UAS-detection systems consequently does not violate the Pen-Trap Statute. For similar reasons, using passive EO/IR UAS-detection systems does not violate the Wiretap Act. Such systems passively absorb visible and infrared light, translate that light into a continuous sequence of images, and evaluate those images to capture drone motions or heat signatures—they do not intercept wire, oral, or electronic communications transmitted by radio wave. *See supra* Part I.C.2.[42]

Active EO/IR Systems. LiDAR is an active UAS-detection system that operates in the near-infrared range. *See supra* Part I.C.2. A transmitter emits light pulses, and its receiver absorbs those reflected light pulses. While LiDAR's light pulses can transmit information, these systems generate their own emissions. They do not record, decode, or capture the dialing, routing, addressing, or signaling information of another party's communication. *See* 18 U.S.C. § 3127(3)–(4).[43] LiDAR likewise does

---

[41] Infrared cameras can possibly identify fiberoptic cables attached to UAS because fiberoptic cables transmit information via near-infrared light pulses. *See* Braszko. But even if these cameras could one day record, decode, or capture the actual signaling information transmitted by these light pulses, they would still not be installed on, attached, or applied to the fiberoptic cable, which is the "facility" serving as the conduit for the UAS communications. The Pen-Trap Statute consequently would not prohibit their use.

[42] UAS could hypothetically use visible or infrared light to communicate by, for example, Morse code or another encoded communication scheme. This would count as an electronic communication. *See* 18 U.S.C. § 2510(12) (defining "electronic communication" to include signals transmitted by photoelectronic systems). Whether an optoelectronic UAS-detection system "intercepts" such communications could depend on (1) whether the government obtained the contents of the communication, and (2) whether the UAS was configured so that the communication was readily accessible to the general public. We need not address these hypothetical scenarios now because those who deploy optoelectronic UAS-detection systems in the normal course of operations do not intentionally intercept any such electronic communications—they instead intend to identify UAS by movement or heat signature. *See supra* Part I.C.2. The Wiretap Act consequently would not apply under such circumstances. *See* 18 U.S.C. § 2511(1); *Wiretapping and Eavesdropping* § 3:3.

[43] While an Integrated Sensing and Communication ("ISAC") LiDAR device can transmit data to other devices via the same light pulses the ISAC LiDAR uses for ranging purposes, the ISAC LiDAR never records, decodes, or captures its own DRAS information or intercepts its own content. Even if it did—or even if it received DRAS information or content from a second LiDAR device that is part of a C-UAS LiDAR array—it is not "attached or applied" to a "facility," *see supra* Part II.A.2, and it is a

not intercept any communication because it does not transmit or access communicative content of any type. *See id.* § 2510(4), (8). Its use violates neither the Pen-Trap Statute nor the Wiretap Act.

C.

Passive Radar. Passive radar operates in the radio spectrum, employing two receivers: one that absorbs original radio waves from a transmission source, and one that absorbs those radio waves after they reflect off airborne objects. *See supra* Part I.C.3. At no point do passive radar systems "record[] or decode[]" the "signaling information" embedded on the reflected radio waves. 18 U.S.C. § 3127(3). And while passive radar systems do "capture[] the incoming . . . impulse[]" (the radio wave), they do not use the radio wave to identify any "dialing, routing, addressing, [or] signaling information reasonably likely to identify the source" of the radio transmission. *Id.* § 3127(4). Such systems use only the physical properties of the waves to identify the objects off which those waves reflect. A passive radar therefore does not fall within the definition of "pen register" or "trap and trace device." Its use consequently does not violate the Pen-Trap Statute.

Neither does passive radar violate the Wiretap Act. While the receiver absorbs radio waves emitted by other sources, it does not access or acquire any electronic communication's *contents—i.e.*, the "information concerning the substance, purport, or meaning of th[e] communication." *Id.* § 2510(8). It therefore does not "intercept" the electronic communication for purposes of the Wiretap Act. *Id.* § 2510(4) (defining "intercept" as "the aural or other acquisition of the *contents*" of an electronic communication (emphasis added)).

Active Radar. Using active radar likewise does not violate the Pen-Trap Statute or the Wiretap Act. Active radar emits and receives its own radio waves. Like the light pulses used by LiDAR, active radar's radio waves contain no dialing, routing, addressing, or signaling information—they contain no information whatsoever. Active radar is therefore not a pen-trap device because it does not record, decode, or capture any information. Nor does it intercept any electronic communication.[44]

---

party to the communication, *see* 18 U.S.C. § 2511(2)(d). It therefore still would not violate the Pen-Trap Statute or Wiretap Act.

[44] Before deploying any UAS-detection system that emits radio waves, SLTT law-enforcement agencies must obtain FCC approval. *See* 91 Fed. Reg. at 41468.

D.

Radiofrequency detection presents a closer question. But we conclude that spectrum monitoring and the interception of remote-identification transmissions do not violate either the Pen-Trap Statute or the Wiretap Act. We also provide guidance regarding radiofrequency-detection devices that engage in protocol decoding or similar signal analysis to acquire the contents of communications, which may in some circumstances violate the Wiretap Act.

1.

Radiofrequency-detection systems can identify UAS using spectrum monitoring to detect and analyze emissions from C2 and other UAS communications links. But their use does not violate the Pen-Trap Statute because they are not "attached or applied" to a "facility."

Some might argue that, because a radiofrequency-detection system can triangulate the position of the unmanned aircraft or ground control station, the system arguably falls within the definition of a trap-and-trace device. That is because it captures "incoming electronic . . . impulses" (the radio waves sent by the unmanned aircraft or ground control station) "which identify . . . signaling information" (the frequency patterns, modulation techniques, and timing sequences used to establish the relevant UAS communication link). 18 U.S.C. § 3127(4). The system analyzes these signal properties to identify the radio waves as UAS communications and then triangulates the location of the UAS or ground control station emitting the radio waves. The "signaling information" identified by capturing the "electronic . . . impulses" is therefore "reasonably likely to identify the source of [the] . . . electronic communication" (the unmanned aircraft or ground control station). *Id.*

But while radiofrequency-detection systems may be "applied" to radio waves, radio waves are not "facilities" for purposes of the Pen-Trap Statute. Recall that a "facility" to which a pen-trap device can be attached must be infrastructure that facilitates the transmission of a wire or electronic communication—or, more accurately, the electronic or other impulses that compose the communication—between end-user devices. Radio waves do not readily fit this definition. They are not infrastructure (whether physical or digital), nor do they facilitate the transmission of electronic or other impulses between end-user devices. Rather, radio waves are the "other impulses" transmitted by the end-user device (the

ground control station or the unmanned aircraft). *See id.* For the reasons explained earlier in Part II.A.2.c, radio waves are not a "facility" within the meaning of the Pen-Trap Statute, and thus spectrum monitoring through radiofrequency-detection systems does not violate that statute.

This argument applies with equal force to UAS emissions from beyond-line-of-sight communications, such as those utilizing satellites or 5G wireless broadband mobile-communication networks. So long as the radiofrequency-detection device is monitoring the spectrum—that is, so long as it is applied to radio waves alone, *see* Brungardt & Carraway at 64—the use of such a device would not violate the Pen-Trap Statute. But if a device or process were attached or applied to a "facility," such as a cellular network's infrastructure, the use of the device would likely violate the Pen-Trap Statute.

Having concluded that the Pen-Trap Statute does not prohibit spectrum monitoring, we must now consider the Wiretap Act. Although radiofrequency-detection devices capture a communication link's electronic emissions, they do not acquire the contents of those emissions. That is, such devices do not extract "any information concerning the substance, purport, or meaning of" the communication conveyed by the electronic emissions. 18 U.S.C. § 2510(8). Radiofrequency-detection systems that are engaged in spectrum monitoring thus do not "intercept" UAS electronic communications, and their deployment does not violate the Wiretap Act. *See id.* § 2510(4).

2.

FAA-required remote-identification broadcasts are transmitted by radio wave and are therefore "electronic communications." 18 U.S.C. § 2510(12).[45] Radiofrequency-detection systems that capture this

[45] To broadcast remote identification, UAS manufacturers and operators install a transmitter on their UAS. ECPA excludes from the definition of "electronic communication" "any communication from a tracking device," as defined in 18 U.S.C. § 3117. 18 U.S.C. § 2510(12)(C). While § 3117 broadly defines "tracking device" as "an[y] electronic or mechanical device which permits the tracking of the movement of a person or object," *id.* § 3117(b), courts have interpreted this provision in the light of the preceding subsection, which clarifies that courts can include in "a warrant or other order for the *installation* of a mobile tracking device" authorization to use that device within or outside of the court's jurisdiction so long as "the device is *installed* in" the court's jurisdiction, *id.* § 3117(a) (emphasis added); *see also Wiretapping and Eavesdropping* § 30:3 & n.3 (citing *United States v. Ackies*, 918 F.3d 190 (1st Cir. 2019); *United States v. Bansal*, 663 F.3d 634 (3d Cir. 2011); *United States v. Berkos*, 543 F.3d 392 (7th Cir.

information thus fall within the definition of "trap and trace devices" because they capture incoming UAS-transmitted DRAS information, such as MAC addresses and SSIDs. *See* 18 U.S.C. § 3127(4); Aouladhadj et al., 23 Sensors at 10–11. But these systems are not attached or applied to a facility. Like spectrum-monitoring equipment, these systems are only applied to "impulses" (radio waves). *See supra* Part III.D.1. Their use therefore does not violate the Pen-Trap Statute.

For purposes of the Wiretap Act, the "content" of a UAS remote-identification communication—that is, the "information concerning the substance, purport, or meaning of th[e] communication," 18 U.S.C. § 2510(8)—includes the UAS's remote-identification serial number, the location of the control station, and the location, velocity, and emergency status of the unmanned aircraft. After all, that is the substantive information that the UAS is attempting to convey to the receiver. Because radiofrequency-detection systems "intercept" these communications and acquire their content "through the use of an[] electronic . . . device," *id.* § 2510(4), those interceptions are unlawful unless an exception applies. Because remote-identification broadcasts currently operate on Bluetooth advertising and local Wi-Fi, that exception is found in § 2511(2)(g)(i).

In the Ninth Circuit, remote-identification broadcasts will be considered non-radio electronic communications. The FAA requires remote-identification broadcasts to occur on a "non-proprietary broadcast specification," 14 C.F.R. § 89.310(g)(1), so that their contents will "be available to most personal wireless devices within range of the broadcast," FAA Rule Summary at 1. In other words, the remote-identification broadcast is transmitted by an electronic communication system—

2008)). Courts have thus concluded that a "tracking device" only includes devices that are "installed" by the government. *Ackies*, 918 F.3d at 199. Because the government does not install transmitters on private UAS, we continue to analyze remote-identification broadcasts as "electronic communications" that are subject to the Pen-Trap Statute and Wiretap Act. *See* 18 U.S.C. §§ 2510(12), 2511(1)(a), 3121(a), 3127(3)–(4).

But even if remote-identification transmitters were "tracking devices," the government could still intercept the contents of their communications. That is because, as a tracking device, the transmitter's communications would not be "electronic communications" and would therefore not be subject to the Pen-Trap Statute or Wiretap Act's dictates. *See* 18 U.S.C. § 2510(12)(C). The only limitation on the interception of such communications would be the Fourth Amendment. And UAS users do not have a reasonable expectation of privacy in the contents of their remote-identification broadcasts. *See Brennan v. Dickson*, 45 F.4th 48, 61 (D.C. Cir. 2022) ("[D]rone pilots generally lack any reasonable expectation of privacy in the location of their drone systems during flight.").

Bluetooth advertising and local Wi-Fi—that incorporates particular elements that make the remote-identification broadcast's contents easily obtainable by any individual. Interception would therefore be authorized because the broadcast is a readily accessible, non-radio electronic communication under § 2511(2)(g)(i). *See supra* Part II.B.2.

If Bluetooth advertising and local Wi-Fi remote-identification broadcasts are "radio communications" (*contra Joffe I*, 729 F.3d at 1270), they could likewise be lawfully intercepted under § 2511(2)(g)(i) because such communications do not fit within any of the five categories listed in § 2510(16). *See* 18 U.S.C. § 2510(16); *supra* Part II.B.1.

First, Bluetooth advertising and local Wi-Fi remote-identification broadcasts are not "scrambled or encrypted." 18 U.S.C. § 2510(16)(A). True, all communications sent via Bluetooth advertising and local Wi-Fi undergo a process known as "data whitening," which shuffles the transmitted data bits (the zeros and ones that communicate the message) to optimize the radiofrequency spectrum and prevent signal degradation. *See* Nthatisi Hlapisi, *Whitening Filters Help Low-Power Radios Tackle Issues Caused by Long Identical Bit Sequences*, All About Circuits (Aug. 2, 2023), https://perma.cc/F3BT-RSK4. Although this process is sometimes called "scrambling," *see id.*, it does not constitute "scrambl[ing]" within the meaning of § 2510(16)(A). Dictionaries from the time of the Wiretap Act's enactment define "scramble" as "to make (a radio or telephonic message) incomprehensible to interceptors by systematically changing the transmission frequencies." *Random House 1987* at 1720; *see also Webster's Third 1993* at 2038 (defining "scramble" as "to make (a telephonic or radio message) unintelligible to interceptors by disarranging the frequencies of the transmission").[46] Data whitening falls outside of this definition, as it only rearranges the bits

[46] Members of Congress appear to have had such a definition in mind when they discussed the term:

> As specified in paragraph (A) of proposed subsection 2510(16), scrambled or encrypted radio communications are not readily accessible to the general public. The terms are used in their technical sense. To "encrypt" or to "scramble" means to convert the signal into unintelligible form by means intended to protect the contents of a communication from unintended recipients. Methods which merely change the form of a plaintext message, e.g., a device which converts an analog signal to a digital stream, does not provide "encryption" within the meaning of this bill.

Wiretapping and Eavesdropping § 2:144 n.2 (quoting S. Rep. No. 99-541, at 15).

within a data packet; it has no effect on the transmission frequency. *See generally* Hlapisi.

Even if "scrambled" in § 2510(16) were not limited to changing transmission frequencies, statutory text and context confirm that it must refer, at most, to a radio communication transmitted by cryptographic means designed to protect privacy. Section 2510(16)(A) pairs "scrambled" with "encrypted"—another cryptographic technique. *See* 18 U.S.C. § 2510(16)(A); *Random House 1987* at 641 (defining "encrypt" as "to encipher or encode"); *Webster's Third 1993* at 747 (same). Section 2510(16)(B) similarly protects radio communications "transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication." 18 U.S.C. § 2510(16)(B). In each case, the radio communication is transmitted in a manner designed to make it more difficult for the general public to intercept. Interpreted in view of the surrounding words and context, *see Jarecki*, 367 U.S. at 307, "scrambled" here at most refers to a radio communication transmitted through a cryptographic technique that renders its contents more difficult to intercept, *see, e.g.*, *The American Heritage Dictionary of the English Language* 1574 (5th ed. 2016) (defining "scramble," more broadly than the contemporary technical definitions, as "[t]o distort or garble (a signal) so as to render it unintelligible without a special receiver").

Far from being a cryptographic technique, data whitening makes radio communications *easier* to intercept—both because it optimizes the communication stream, *see* Hlapisi, and because the protocol required to unshuffle whitened bits is made public knowledge by design, *see, e.g.*, *IEEE 802.11-2024* at 3317 (2024); Bluetooth, *Bluetooth Core Specifications* 541–42 (6th ed. 2024). The protocol to unshuffle whitened data is built into every modern smartphone and laptop, which allows such devices to communicate readily with other Wi-Fi or Bluetooth-enabled devices. *See, e.g.*, Hlapisi; *IEEE 802.11-2024* at 3317; Bluetooth at 541–42. Because data whitening serves no cryptographic function, communications transmitted via standard Wi-Fi and Bluetooth are not "scrambled" for purposes of § 2510(16)(A).[47]

[47] The fact that data whitening does not qualify a radio communication sent by Wi-Fi or Bluetooth for protection does not mean that all Wi-Fi and Bluetooth transmissions are readily accessible to the general public and therefore may be legally intercepted under § 2511(2)(g)(i). Modern Wi-Fi and Bluetooth typically incorporate a series of security measures, including passwords and encryption, which would preclude the

Second, Bluetooth advertising and local Wi-Fi remote-identification broadcasts are not "transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication." 18 U.S.C. § 2510(16)(B). As noted, the FAA requires that the broadcast occur on a "non-proprietary broadcast specification," 14 C.F.R. § 89.310(g)(1), so that their contents will "be available to most personal wireless devices within range of the broadcast," FAA Rule Summary at 1. Bluetooth advertising and local Wi-Fi are the current transmission method of choice precisely because they fit this bill.

Third, Bluetooth advertising and local Wi-Fi remote-identification broadcasts are not "carried on a subcarrier or other signal subsidiary to a radio transmission." 18 U.S.C. § 2510(16)(C). Modern Wi-Fi does employ a process called orthogonal frequency-division multiple access ("OFDMA"), which divides a single radiofrequency channel into hundreds of "subcarriers." *See* ScienceInsights, *What Is OFDMA in WiFi and How Does It Work?* (Mar. 12, 2026), https://perma.cc/Z72R-U926. The use of the term "subcarrier" could lead some to mistakenly conclude that modern Wi-Fi falls into § 2510(16)(C), which identifies radio communications "carried on a subcarrier or other signal subsidiary to a radio transmission" as not readily accessible to the public. But as used in § 2510(16)(C), "subcarrier" refers to a separate radiofrequency that "rides along" with a primary radiofrequency carrier. *See* Bruce E. Boyden, *Why Google's Wi-Spy Argument is Stronger than It First Appears*, Marq. U. L. Sch. Blog (Aug. 19, 2013), https://perma.cc/NCP3-C9QB; *see also Wiretapping and Eavesdropping* § 2:144 n.3 (identifying "data and background music services carried on FM subcarriers" and "data carried on the Vertical Blanking Interval . . . of a television signal" as examples of radio communications protected under § 2510(16)(c) (quoting S. Rep. No. 99-541, at 15)); *Webster's Third 1993* at 2273 (defining "subcarrier" as "a low-frequency carrier in an electronic system (as a telemetering system or a multi-channel radio system) used to modulate a main carrier and often being itself modulated to carry information"). The so-called subcarriers in OFDMA-equipped Wi-Fi, however, do not "ride along" with any primary radiofrequency carrier. They *are* the primary radiofrequency carrier.

---

application of that exception. *See* 18 U.S.C. § 2510(16)(A); *supra* Part II.B.2. Remote-identification broadcasts, by contrast, are legally *prohibited* from employing such security measures. *See* 14 C.F.R. § 89.310(g)(1), (h)(5).

Fourth, Bluetooth advertising and local Wi-Fi remote-identification broadcasts are not "transmitted over a communication system provided by a common carrier." 18 U.S.C. § 2510(16)(D). Bluetooth advertising and local Wi-Fi instead provide short-range device-to-device connections that do not require the intervention of an internet service provider or a common carrier such as a telecommunications service provider.

Fifth, such broadcasts are not transmitted on the frequencies identified in § 2510(16)(E). Bluetooth advertising utilizes the 2.4 GHz ISM band. And local Wi-Fi utilizes the 2.4 GHz and 5 GHz ISM bands.

Regardless of whether "radio" is defined in a common or technical sense, then, federal and SLTT officials may use radiofrequency-detection systems outside the statutory C-UAS authorities to capture UAS remote-identification broadcasts sent via Bluetooth advertising or local Wi-Fi without violating the Wiretap Act.[48]

3.

Radiofrequency-detection systems that engage in protocol decoding or other signal analysis that "extracts information directly from the communication stream" can acquire DRAS information and contents of communications. Drone Warfare, *RF Drone Detection* § 1.3. Like systems that capture remote-identification information, protocol-decoding

[48] Remote identification may also fall within § 2511(2)(g)(ii)(I)'s exception for radio communications transmitted "by any station for the use of the general public." Although the Wiretap Act does not define "station," the Communications Act of 1934 defines that term to mean "a station equipped to engage in radio communication or radio transmission of energy." 47 U.S.C. § 153(42). The FCC further defines "[s]tation" to mean "[o]ne or more transmitters or receivers or a combination of transmitters and receivers, including the accessory equipment, necessary at one location for carrying on a radiocommunication service." 47 C.F.R. § 2.1(c). The FCC also defines "[r]adiocommunication [s]ervice" as a "service . . . involving the transmission, emission and/or reception of radio waves for specific telecommunication purposes." *Id.* And it defines "[t]elecommunication" as "[a]ny transmission, emission or reception of signs, signals, writings, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems." *Id.*

A remote identification is a "station" under FCC's definition because it is a "transmitter" that emits radio waves for the purpose of conveying information. *See* 14 C.F.R. §§ 89.305, 89.310(h)(5), 89.315. And that transmission is required for both public and private airspace awareness—*i.e.*, the transmission is "for the use of the general public." 86 Fed. Reg. 4390, 4396 (Jan. 15, 2021) ("Remote identification is the capability of an unmanned aircraft in flight to provide identification, location, and performance information that people on the ground and other airspace users can receive.").

systems are pen-trap devices because they record, decode, and capture DRAS information transmitted between the ground control station and unmanned aircraft. *See* 18 U.S.C. § 3127(3)–(4). And for the same reason, their use does not violate the Pen-Trap Statute: These systems are not attached or applied to a facility within the meaning of the Pen-Trap Statute.

But unless a Wiretap Act exception applies, using such systems will often violate the Wiretap Act and require federal and SLTT law-enforcement officers to operate within the statutory C-UAS authorities.[49] We provide some general guidance here.[50]

---

[49] For the avoidance of doubt, using electronic emissions to triangulate an unmanned aircraft's location and infer its velocity does not implicate the Wiretap Act. *See supra* Part III.D.1. In that scenario, multiple devices capture the radio waves transmitted by an unmanned aircraft. Each device produces "a Line of Bearing (LOB): a vector pointing toward the transmitter, but with no information about distance or altitude. Networks of three or more sensors with favorable geometry can triangulate this to a fix, calculating latitude, longitude, and altitude for both drones and their operators." Drone Warfare, *RF Drone Detection* § 2.1 (emphasis omitted). Multiple fixes over time allow the system to infer the unmanned aircraft's velocity. Importantly, such devices complete this process without ever acquiring the contents of the communications encoded on the captured radio waves. *See* 18 U.S.C. § 2510(4).

By contrast, a remote-identification broadcast is an electronic communication whose content includes, among other information, the location and velocity of the unmanned aircraft. *See supra* Part III.D.2. An unmanned aircraft similarly might transmit to its ground control station an electronic communication that identifies the UAS's location and velocity—which, again, constitutes the content of the communication: It is the very information the UAS seeks to convey to the ground control station. A radiofrequency-detection device that not only captures radio waves containing this information but also subsequently looks at it has thus acquired the "contents" of an electronic communication, 18 U.S.C. § 2510(4), thereby implicating the Wiretap Act, *see id.* § 2511(1)(a). In this way, radiofrequency-detection devices can acquire the same information (the unmanned aircraft's location and velocity), but the Wiretap Act's applicability depends on the source of the information.

[50] Military personnel engaged in radiofrequency detection and acting in a non-law-enforcement capacity should exercise special caution, as the guidance in this section of our opinion may not fully apply to such personnel. Federal law prohibits the disclosure and use of intercepted radio communications "[e]xcept as authorized by" the Wiretap Act. 47 U.S.C. § 605(a). The Wiretap Act expressly permits "investigative or law enforcement officer[s]" to disclose or use lawfully intercepted electronic communications. 18 U.S.C. § 2517(a)–(b). But many military personnel will not qualify as "investigative or law enforcement officer[s]." *Id.* § 2510(7) (defining "investigative or law enforcement officer" as "any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for

Courts in the Ninth Circuit will consider UAS communications to be non-radio "electronic communications." *See Joffe II*, 746 F.3d at 928. Such communications are lawfully intercepted under § 2511(2)(g)(i) only if the UAS communication architecture—the "electronic communication system"—incorporates elements that make the communication link's contents easily obtainable by the general public. *See supra* Part II.B.2. This determination, in turn, requires an analysis of each "layer" of the UAS communication architecture: (1) the physical layer, which dictates how data packets are transmitted, *see* Khan at 299; (2) the security protocol, which dictates how data packets are protected, *see* Maresch at 331–32; and (3) the data-framing protocol, which dictates how bits are packaged in data packets, *see id.* at 328; *see also generally* Roxxanne White & Michael Bragg, *Radio Frequency 101: Can You Really Hack a Radio Signal?*, Carnegie Mellon U. (June 16, 2025), https://perma.cc/5VM8-KPPS. If the communication architecture at any level incorporates a reasonable attempt to prevent access to its communications, *see supra* Part II.B.2, then the system is not "configured so that [the transmitted] electronic communication is readily accessible to the general public," 18 U.S.C. § 2511(2)(g)(i).

Start with the physical layer. To intercept a communication, a radio-frequency-detection device must first capture and demodulate the radio wave that carries the communication. *See* Khan at 305; Lamia Alhoraibi et al., *Physical Layer Authentication in Wireless Networks-Based Machine Learning Approaches*, 23 Sensors, no. 4, 2023, at 5. If a UAS employs open-standard wireless communication technologies that do not require private parameters, such as unsecured Wi-Fi and Bluetooth, demodulation is straightforward because the exact parameters required for demodulation have been intentionally disclosed to the public. *See* White

---

offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses"). And at least the Sixth Circuit has held that, although the exceptions in § 2511(2)(g) permit an individual who is not an investigative or law-enforcement officer to intercept an electronic communication, they do not permit that individual to use or disclose the intercepted communication for purposes of 47 U.S.C. § 605. *See Cafarelli v. Yancy*, 226 F.3d 492, 499 (6th Cir. 2000). In at least some jurisdictions then, military personnel who are acting outside the statutory C-UAS authorities and are not "investigative or law enforcement officer[s]" might be subjected to civil suits under 47 U.S.C. § 605(e)(3) for disclosing or using the contents of intercepted UAS communications, even where the interception itself was lawful under 18 U.S.C. § 2511(2)(g).

& Bragg; *IEEE 802.11-2024* at 3317; Bluetooth at 541–42. The use of voluntarily disclosed parameters indicates that the system is configured to make its communications readily accessible to the general public. By contrast, UAS that employ proprietary wireless communication technologies whose signal parameters and underlying modulation techniques have been withheld from the public, such as DJI's Lightbridge or OcuSync, demonstrate the requisite "indicia of intended privacy" to remove them from § 2511(2)(g)(i)'s exception. *hiQ Labs*, 31 F.4th at 1200. Similarly, while ExpressLRS is an open-source wireless control protocol, it relies on LoRa, a proprietary modulation technology, in addition to private, user-input parameters, again representing a reasonable attempt to prevent access to its communications. *See* Gabriel Garcia et al., *Implementation and Analysis of ExpressLRS Under Interference Using GNU Radio*, 10 Procs. 15th GNU Radio Conf., 2025, at *1–3. Such communications are not readily accessible to the general public.

Next, consider the security protocols. *See* Alhoraibi et al., 23 Sensors at 7–8; Maresch at 331–32. If the UAS communication architecture incorporates *any* security measure—such as a password, encryption, or other cryptographic technique—then the system is not configured so that its communications are readily accessible to the public. *See* Maresch at 331–32. Conversely, the absence of security protocols indicates that the electronic communication system is configured to make its communications readily accessible.

Finally, there is the data-framing protocol. A UAS's use of a voluntarily published data-framing protocol, such as ASTM F3411 or Micro Air Vehicle Link (commonly called "MAVLink"), shows that its system is configured to make communications readily accessible to the general public. That is because anyone who knows the protocol can readily parse the bits and convert them back into readable data. Use of a proprietary data-framing protocol, on the other hand, indicates a reasonable effort to prevent access to the system's communications. In that case, the interceptor must reverse-engineer the protocol to parse the bits and convert them into readable data—a process analogous to deciphering the dead language of a lost civilization. *See* Johannes Pohl & Andreas Noack, *Automatic Wireless Protocol Reverse Engineering*, 13 Procs. USENIX Conf. on Offensive Techs., 2019, at 1. Such a configuration precludes the interception of the communication under § 2511(2)(g)(i).

If UAS transmissions are understood to be "radio communications" (*contra Joffe II*, 946 F.3d at 928), the analysis is more straightforward. Does the communication architecture fall within § 2510(16)? If not, then the communication is "readily accessible to the general public." Section 2510(16)(A) addresses the security protocols: If the transmitted data is cryptographically scrambled or encrypted, it is protected against interception unless a different exception applies. Section 2510(16)(B) and (C) address the physical layer: If the radio communication is "transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication" or is "carried on a subcarrier or other signal subsidiary to a radio transmission," then it is likewise protected from interception absent a different exception. Section 2510(16)(D) addresses the communication system itself, prohibiting the interception of communications "transmitted over a communication system provided by a common carrier," which can include, for example, commercial wireless service providers. *See* 47 U.S.C. § 332(c)(1). And § 2510(16)(E) concerns the spectrum on which the communication is transmitted, prohibiting the interception of communications sent on certain regulated frequency bands. Because UAS communications that use standard, unsecured Wi-Fi and Bluetooth communications systems do not fall into these categories, such communications may be intercepted under § 2511(2)(g)(i).[51]

Regardless of whether the Pen-Trap Statute and Wiretap Act apply, radiofrequency-detection systems that engage in protocol decoding or other signal analysis must always be used consistently with the constitutional protections of the Fourth Amendment, as applicable.

---

[51] We understand that certain DJI-manufactured UAS broadcast an encrypted AeroScope packet that uses a propriety modulation technique designed to be intelligible to DJI-manufactured AeroScope receivers. The AeroScope packet contains data including the UAS's model, location, and other telemetry information. Because AeroScope receivers engage in protocol decoding and decryption only with respect to DJI-manufactured UAS transmitting the AeroScope packet, and because the AeroScope packet is intended for and transmitted specifically to AeroScope users, AeroScope users are "a party to the communication" who may lawfully intercept the AeroScope packet consistent with 18 U.S.C. § 2511(2)(c) and (d). *See In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 143 (3d Cir. 2015). But individuals utilizing systems that employ reverse-engineered encryption keys or other protocol decoding are not "part[ies] to the communication" and therefore may not benefit from this exception. 18 U.S.C. § 2511(2)(c), (d).

IV.

Based on the information we have been given and subject to the limitations we have identified, the four categories of UAS-detection systems you have asked us to assess do not typically violate either the Pen-Trap Statute or the Wiretap Act. But we caution that using radiofrequency-detection systems to obtain the contents of UAS communications may violate the Wiretap Act except as described in Part III.D.3. UAS-detection systems operating in the manner that we have described may therefore be deployed by federal and SLTT agencies without relying on the statutory reliefs from Pen-Trap Statute and Wiretap Act liability found in 6 U.S.C. § 124n, 10 U.S.C. §§ 130i and 6227, and 50 U.S.C. § 3515a.

T. ELLIOT GAISER
Assistant Attorney General
Office of Legal Counsel