Congressional Research Service
Informing the legislative debate since 1914

MEMORANDUM March 1, 2021

To: Senator Ron Wyden
Attention: [redacted]

From: [redacted] Legislative Attorney, [redacted]

Subject: **Analysis of 18 U.S.C. § 2511(2)(f)**

This memorandum responds to your request for an analysis of 18 U.S.C. § 2511(2)(f), a provision of the Electronic Communications Privacy Act (ECPA), which describes how that statute and other federal surveillance laws apply to certain foreign intelligence activities. Specifically, you asked how Section 2511(2)(f) might apply to voluntary disclosures of communications metadata from communications providers to a federal agency. Before addressing Section 2511(2)(f) in particular, this memorandum first provides a brief history and overview of federal surveillance law, including both constitutional and statutory restrictions.

Background

The Fourth Amendment to the U.S. Constitution provides a right "of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[1] Government action constitutes a search when it intrudes upon a person's "reasonable expectation of privacy," which requires both that an "individual manifested a subjective expectation of privacy in the searched object" and that "society is willing to recognize that expectation as reasonable."[2] As a general rule, the Fourth Amendment requires the government to demonstrate "probable cause" and obtain a warrant issued by a "neutral and detached magistrate"[3] before conducting a search.[4]

The U.S. Supreme Court first held that government recording or interception of electronic communications is a search for purposes of the Fourth Amendment in its 1967 decision in *Katz v. United States*.[5] By contrast, the Supreme Court has not historically applied Fourth Amendment protections to the

[1] U.S. CONST. amend. IV.

[2] Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing California v. Ciraolo, 476 U.S. 207, 211 (1986)).

[3] Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972).

[4] *See, e.g.*, Atwater v. City of Lago Vista, 532 U.S. 318, 354 (2001) (recognizing a warrant exception for arrest of an individual who commits a crime in an officer's presence, as long as the arrest is supported by probable cause). Probable cause is "a fluid concept—turning on the assessment of probabilities in particular factual contexts." Illinois v. Gates, 462 U.S. 213, 232 (1983). For example, for issuance of a search warrant, probable cause requires an issuing magistrate to determine, based on specific evidence, whether there exists a "fair probability" that, for example, an area contains contraband. *Id.* at 238.

[5] Katz v. United States, 389 U.S. 347, 353 (1967), *overruling* Olmstead v. United States, 277 U.S. 438 (1928).

government's collection of metadata concerning electronic communications. For example, in 1979, the Supreme Court held that the installation and use of a pen register—a device used to capture telephone numbers dialed—does not constitute a Fourth Amendment search.[6] The Court reasoned that individuals have a lesser expectation of privacy with regard to information held by third parties.[7] Lower courts have applied this same reasoning to deny Fourth Amendment protections for non-content data associated with modern communications, such as the to/from address line in an email,[8] although the content of communications—for example, the body of an email—is protected by the Fourth Amendment.[9] However, in 2018, the Supreme Court held that obtaining seven days of historical location information from cellular telephone providers also constituted a Fourth Amendment search.[10] In extending Fourth Amendment protections to such location information, the Court reasoned that, given the ubiquity of cell phones and the fact that cell phone users can transmit their location simply by possessing their phones, "[o]nly the few without cell phones could escape this tireless and absolute surveillance" by law enforcement.[11]

These judicial developments have also prompted Congressional responses. Following *Katz v. United States*, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[12] which generally prohibits government wiretaps except where sanctioned by a court order or warrant supported by probable cause. The ECPA amended Title III in 1986, adding the Stored Communications Act (SCA) to regulate the privacy of stored communications and the government's access to such communications.[13] ECPA also added provisions governing the installation and use of pen registers and trap-and-trace devices (Pen Register statute).[14]

The SCA generally prohibits a provider of a remote computing service (RCS) or an electronic communication service (ECS) to the public from disclosing a record or other information to the government except pursuant to a subpoena or court order.[15] The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[16] An RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[17] Federal courts have generally agreed that providers of telephone, cellular, email, and internet services are either ECS or RCS providers covered by the prohibition against disclosing communications records or other information to a governmental entity.[18] This prohibition does not apply to entities that are not ECS or RCS providers.[19]

---

[6] Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

[7] *Id.* at 744.

[8] United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2007).

[9] United States v. Warshak, 631 F.3d 266 (10th Cir. 2010).

[10] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[11] *Id.* at 2218.

[12] Pub. L. No. 90-351, 82 Stat. 197, 211.

[13] 18 U.S.C. §§ 2701–2713.

[14] *Id.* §§ 3121–3127.

[15] *Id.* § 2702(a).

[16] *Id.* § 2510(15) (incorporated into the SCA by reference pursuant to 18 U.S.C. § 2711(1)).

[17] *Id.* § 2711(2).

[18] Hately v. Watts, 917 F.3d 770 (4th Cir. 2019); Brown Jordan Int'l, Inc. v. Carmicle, 846 F.3d 1167 (11th Cir. 2017); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 902 (9th Cir. 2008), *rev'd and remanded on other grounds sub nom.* City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010).

[19] *See, e.g.*, Keithly v. Intelius Inc., 764 F. Supp. 2d 1257, 1271-72 (W.D. Wash. 2011) (holding that online provider of background checks and other information services did not violate SCA when disclosing customer billing information to third party because it does not provide users with the ability to send or receive communications and is therefore not an ECS).

Other companies that carry internet communications between ECS providers, such as internet backbone providers, would also likely qualify as an ECS provider, but there may be questions regarding whether those backbone providers are providing an ECS *to the public*, rather than only to those telecommunications companies that interface with end users. CRS did not identify any published court decision that addresses this precise question. However, when evaluating whether an ECS or RCS is providing services to the public, at least one court has held that the term "public" unambiguously refers to the "community at large."[20] That court also distinguished between electronic communications services that are provided "for public use" as opposed to "proprietary" systems, such as those used "by private companies for internal correspondence."[21] For example, a chemical company that provided email access to a contractor for the purposes of communication with other employees was not providing an ECS to the "public" notwithstanding the fact that the contractor could use that email system to communicate with third parties.[22]

An internet backbone service provider would not appear to be providing the same kind of "proprietary" service that this court distinguished from a "public" purpose because the backbone carries communications that are not the internal communications of the companies to which it provides backbone services. Additionally, while the "community at large" may not be direct customers of a backbone internet provider, that backbone provides the "community at large" with the ability to communicate across the internet. Lastly, excluding backbone internet service providers from the SCA's prohibition on disclosures would create a significant loophole in a statute that was enacted to protect the privacy of internet and telephone communications. Therefore, although the statute might be more clearly written to expressly include such backbone providers, it appears reasonable to interpret such providers as providing an ECS to the public.

Relatedly, Section 705 of the Communications Act of 1934 also regulates persons "receiving, assisting in receiving, transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio." It then prohibits such persons from disclosing the "existence, contents, substance, purport, effect, or meaning" of such communications except in authorized situations, including in response to a subpoena issued by a court of competent jurisdiction or on demand of other lawful authority.[23]

Section 2511(2)(f)

ECPA and the SCA primarily concern government surveillance or access to stored communications for *law enforcement* purposes. As originally enacted, Title III included a disclaimer expressly stating that nothing in Title III was intended to limit the President's constitutional power to gather necessary intelligence to protect the *national security*.[24] In 1978, Congress enacted the Foreign Intelligence Surveillance Act (FISA) to regulate electronic surveillance conducted for national security or foreign

[20] Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (citing dictionary definition of "public").

[21] *E.g., id.* (citing legislative history of ECPA at S. REP. NO. 99-541, at 8 (1986)). *See also* Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1226 (Aug. 2004) (concluding that an ECS does not provide services to the public where the provider has a special relationship, such as employment, with the user and the service is provided for "work-related purposes" or "official government business").

[22] *Andersen Consulting LLP*, 991 F. Supp. at 1043. The prohibition in Section 705 is separate from the telecommunications duty under Section 222 of the Communications Act to protect the confidentiality of customer proprietary network information (CPNI). *See* 47 U.S.C. § 222; 47 C.F.R. §§ 64.2001–64.2011. However, some information that would be protected as CPNI also appears to be protected under Section 705. For example, CPNI is defined to include, among other things, the quantity, destination, location, and amount of use of a telecommunications service, which would also likely qualify as information about the existence of a communication under Section 705.

[23] 47 U.S.C. § 605.

[24] 18 U.S.C. § 2511(3) (1977).

intelligence purposes. Like Title III, FISA includes a procedure for the government to obtain a court order, supported by probable cause, authorizing electronic surveillance for foreign intelligence purposes. FISA also repealed the national security disclaimer in Title III, replacing it with a more limited disclaimer to preserve "certain international signals intelligence activities currently engaged in by the National Security Agency [(NSA)] and electronic surveillance conducted outside the United States."[25]

This more limited waiver is the forerunner to Section 2511(2)(f), which currently provides:

> Nothing contained in this chapter [Title III] or chapter 121 [the SCA] or 206 of this title [the Pen Register statute], or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of [FISA], and procedures in this chapter or chapter 121 and [FISA] shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.[26]

Accordingly, Section 2511(2)(f) identifies two broad categories of government activities that are exempt from Title III, the SCA, the Pen Register statute, and section 705 of the Communications Act of 1934:[27] (1) the "acquisition by the United States Government of foreign intelligence information from international or foreign communications"; and (2) "foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system." These two categories are further qualified so that the exception only applies if: (3) the acquisition or the foreign intelligence activity is not "electronic surveillance" as defined under FISA; and (4) an "exclusivity" clause states that ECPA, the SCA, and FISA shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, and electronic communications may be conducted. Each of these clauses is discussed in more detail below.

(1) International and Foreign Communications

The first category of government conduct covered by Section 2511(2)(f) is described as "the acquisition . . . of foreign intelligence information from international or foreign communications."[28] The term "acquisition" is central to this clause's meaning. That is, if the government's conduct is not an acquisition, then that conduct is not captured by this clause. The term "acquisition" is not defined by either ECPA or FISA.[29] The Supreme Court has said that when a statutory term is not defined, it generally should be given its "ordinary meaning"—typically, its dictionary definition.[30] However, a term's ordinary meaning may not apply if the word or phrase is a term of art because it has a technical or settled meaning in the relevant subject area or legal field.[31]

---

[25] H.R. REP. NO. 95-1283, at 100; *see also* S. REP. NO. 95-701, at 71. *See also* Alberto Gonzales, Attorney General of the United States, Prepared Statement (Feb. 6, 2006) (stating "Congress did not intend FISA to regulate certain communications intelligence activities of the NSA, including certain communications involving persons in the United States" as evidenced by Section 2511(2)(f)), *available at* https://www.justice.gov/archive/ag/speeches/2006/ag_speech_060206.html.

[26] 18 U.S.C. § 2511(f).

[27] Because CPNI regulations are promulgated under the authority of Section 222 of the Communications Act, and not Section 705, it does not appear that Section 2511(2)(f) would have any effect on the requirements of those regulations.

[28] 18 U.S.C. § 2511(2)(f).

[29] KRIS & WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 7:9 (West 2019).

[30] *See* Taniguchi v. Kan Pac. Saipan, Ltd., 566 U.S. 560, 566 (2012) ("When a term goes undefined in a statute, we give the term its ordinary meaning.").

[31] *See, e.g.*, Arlington Cent. Sch. Dist. Bd. of Educ. v. Murphy, 548 U.S. 291, 297 (2006) (declining to interpret "costs" according

Various dictionaries define "acquisition" broadly as "[t]he process by which one gains knowledge" or "the gaining of possession or control over something."[32] The term "acquisition" is also used in both ECPA and FISA. For example, ECPA defines the term "interception" as "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."[33] Similarly, FISA uses the term "acquisition" throughout its definition of "electronic surveillance," discussed in more detail below. Therefore, the use of the term "acquisition" in Section 2511(2)(f) appears to encompass traditional wiretapping, in which someone listens to or records a live communication.[34] FISA also uses the term "acquired" to refer to information received by the government from persons ordered to produce certain tangible things (albeit in provisions that have since sunset).[35] This suggests that the term "acquisition" as used in Section 2511(2)(f) may also include situations in which the government gains possession of information after it is independently recorded or collected by a third party.[36]

This clause further requires that the acquisition be of "foreign intelligence information from international or foreign communications."[37] The term "foreign intelligence information" is defined under FISA as:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> >
> > (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
> >
> > (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--
>
> > (A) the national defense or the security of the United States; or

---

to its "ordinary usage" as expenses incurred because "'costs' is a term of art that generally does not include expert fees" (internal quotation marks and citation omitted)); Cmty. for Creative Non-Violence v. Reid, 490 U.S. 730, 740 (1989) (noting that the term "scope of employment" is a "widely used term of art in agency law").

[32] *Acquisition*, BLACK'S LAW DICTIONARY (11th ed. 2019); *Acquire*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/acquire (last visited Nov. 9, 2020).

[33] 18 U.S.C. § 2510(4).

[34] *See, e.g.*, United States v. Lewis, 406 F.3d 11, 17 (1st Cir. 2005) (holding that telephone system administrator "*acquired* the contents of [a] conversation when he recorded it" in violation of ECPA (emphasis added)).

[35] 50 U.S.C. § 1861(h).

[36] *See, e.g.*, United States v. Hammond, 286 F.3d 189, 192 (4th Cir. 2002) (describing FBI's receipt of tapes in response to subpoena as "acquisition" in the context of an alleged ECPA violation). *See also* DOD MANUAL 5240.01, at G.2 (Aug. 8, 2016) (establishing procedures for Department of Defense intelligence activities and defining collection as including "information obtained or *acquired by any means, including information that is volunteered to the Component*" (emphasis added)), *available at* https://dodsioo.defense.gov/Portals/46/DoDM%20%205240.01.pdf; Attorney General Jeff Sessions, *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*, at 2 (Mar. 29, 2017) ("Acquisition means the collection by NSA or the Federal Bureau of Investigation (FBI) through electronic means of a non-public communication to which it is not an intended party."), *available at* https://www.dni.gov/files/documents/icotr/51117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf; Attorney General Janet Reno, *Standard Minimization Procedures for Electronic Surveillance Conducted by the National Security Agency (NSA)*, at 2 (July 1, 1997) (same), *available at* https://www.dni.gov/files/documents/0315/Exhibit%20B%20to%20May%2010%202002%20Motion.pdf.

[37] 18 U.S.C. § 2511(2)(f).

(B) the conduct of the foreign affairs of the United States.[38]

Neither ECPA nor FISA statutorily define the term "international communication" or "foreign communication." The House Report accompanying the bill that eventually became FISA uses the term "foreign communication" to refer to communications between persons located outside the United States, while "international communications" refers to communications between someone in the United States and someone abroad.[39] Federal courts do not appear to have addressed, and it may not be clear from the text alone, whether a communication that is made between two persons in the United States, but routed internationally, would qualify as an "international communication" for purposes of Section 2511(2)(f).[40]

(2) Foreign Electronic Communications System

The second category of conduct to which the exception in Section 2511(2)(f) applies is "foreign intelligence activity in accordance with otherwise applicable Federal law involving a foreign electronic communications system."[41] The term "foreign intelligence activity" is not defined, and, given the generic term "activity," could potentially encompass a broad array of conduct. The more limiting phrase in this clause appears to be "involving a foreign electronic communications system." ECPA defines an electronic communications system as "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."[42] Based on the ordinary meaning of "foreign," a foreign electronic communications system appears to refer to such a system that is located outside of the United States.[43] The adjective foreign could arguably also be read to include an electronic communications system that is owned by a foreign company, even if it is located within the United States. However, as discussed in the next section, the applicability of the exception in Section 2511(2)(f) to a domestically located, but foreign owned, electronic communications system may be limited by the carve-out for "electronic surveillance" in Section 2511(2)(f).

(3) FISA Electronic Surveillance

Section 2511(2)(f) provides that governmental conduct covered by the "acquisition" clause or the "activities" clause is covered by its exception, but only if the government "utilize[s] a means other than

---

[38] 50 U.S.C. § 1801(e). ECPA includes a nearly identical definition of foreign intelligence information. *See* 18 U.S.C. § 2510(19).

[39] H.R. REP. NO. 95-1283, at 50–51 (referring to international communications of U.S. persons who are located in the United States in contrast to foreign communications in which a U.S. person is abroad); *see also* Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644, 651 (6th Cir. 2007) (citing orders authorizing the collection of international communications into or out of the United States).

[40] In the context of a different provision of FISA, 50 U.S.C. § 1881a, the NSA has defined "foreign" and "domestic" communications exclusively based on the location of the parties to the communication, regardless of where the communication was routed. *See* Redacted, 2011 WL 10945618, at *17 (Foreign Intel. Surv. Ct. Oct. 3, 2011) (quoting NSA minimization procedures: "Foreign communication means a communication that has at least one communicant outside of the United States" and "[a]ll other communications, including communications in which the sender and all intended recipients are reasonably believed to be located in the United States at the time of acquisition, are domestic communications"). *See also* NSA, UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE 18, at 23 (Jan. 25, 2011) (defining "foreign communication" to mean a communication where at least one communicant is outside of the United States), *available at* https://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

[41] 18 U.S.C. § 2511(2)(f).

[42] *Id.* § 2510(14).

[43] *Foreign*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("Of, relating to, or involving another country."). See also H. REP. NO. 95-1283, at 66 (distinguishing between *U.S.* telecommunications common carriers and those operating in a foreign country).

electronic surveillance as defined in [FISA]."[44] FISA's statutory definition of electronic surveillance includes four categories:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
>
> (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[45]

As noted above, this definition uses the term "acquisition" as its main noun. However, acquisition is qualified by the phrase "by an electronic, mechanical, or other surveillance device." Therefore, some intelligence activities that qualify as "acquisitions" for purposes of Section 2511(2)(f) may not qualify as "electronic surveillance" under FISA because the acquisition is not accomplished through an electronic, mechanical, or other surveillance device. Although FISA does not define this phrase, ECPA provides a definition of "electronic, mechanical, or other device" to mean "any device or apparatus which can be used to intercept a wire, oral, or electronic communication."[46] However, this definition expressly excludes "any telephone or telegraph instrument, equipment or facility, or any component thereof" that is "being used by a provider of wire or electronic communication service in the ordinary course of its business."[47] Additionally, the definitions section of ECPA applies only to that statute, the phrase "electronic, mechanical, or other surveillance device" for purposes of FISA may not be coterminous with the definition of the phrase "electronic, mechanical, or other device" in ECPA.[48]

Additionally, the first, third, and fourth categories of this definition apply only if a person has a reasonable expectation of privacy and the circumstances require a warrant for law enforcement purposes. As discussed above, courts have held that individuals do not have a reasonable expectation of privacy in many types of communications metadata, with the possible exception of extended collection of location information. By contrast, the second category of FISA's definition of electronic surveillance does not require a reasonable expectation of privacy. However, it does require that the acquisition occur within the United States, and is also limited to acquisitions of the contents of *wire communications*. FISA defines wire communications as "any communication *while it is being carried* by a wire, cable, or other like

[44] 18 U.S.C. § 2511(2)(f).

[45] 50 U.S.C. § 1801(f).

[46] 18 U.S.C. § 2510(5).

[47] *Id*.

[48] *See* David S. Kris and J. Douglas Wilson, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 7:10, at n.4 (Sept. 2019) ("FISA surveillance devices need not always be designed primarily for surreptitious use").

connection furnished or operated *by any person engaged as a common carrier* in providing or operating such facilities for the transmission of interstate or foreign communications."[49]

Lastly, FISA defines "contents" of a communication as "any information concerning the identity of the parties to such communication or the *existence*, substance, purport, or meaning of that communication."[50] Notably, the inclusion of "existence" in this list would appear to capture many, if not all, types of communications metadata in FISA's definition of "contents."

(4) Exclusivity Clause

The final clause of Section 2511(2)(f) states that the "procedures in [ECPA] and [FISA] shall be the exclusive means by which electronic surveillance, as defined in section 101 of [FISA] and the interception of domestic wire, oral, and electronic communications may be conducted." It is unclear whether this final clause has a different effect than the earlier clauses. The exclusivity clause is first directed at interception of domestic communications, which would not appear to be affected by the previous disclaimers regarding acquisition of *foreign* and *international* communications or *foreign* intelligence activities directed at foreign electronic communications systems. To the extent the exclusivity clause also discusses electronic surveillance under FISA, such activities are already excluded from the scope of the previous disclaimers, as described above. In 2007, a divided panel of the U.S. Court of Appeals for the Sixth Circuit distinguished the exclusivity clause from the rest of Section 2511(2)(f), noting that it "does not merely disclaim Title III's application" but "prescribes the separate roles of Title III and FISA, rather than the application of Title III alone."[51] However, the Sixth Circuit rejected a broader interpretation of the exclusivity clause offered by plaintiffs challenging certain NSA surveillance programs, in which it was asserted that the exclusivity clause "states that Title III and FISA are together the 'exclusive means' by which the NSA can intercept any communication."[52]

Analysis

This section analyzes how Section 2511(2)(f) would apply to disclosures of communications metadata by U.S. communications providers (such as cellular or landline telephone providers, email providers, internet service providers, and internet backbone providers) to a federal agency in the context of a foreign intelligence investigation.[53] These types of providers would seemingly qualify as an ECS under the SCA, and the SCA generally prohibits an ECS from disclosing customer information to a governmental entity absent a court order or subpoena, unless the exception in Section 2511(2)(f) applies.[54] In the context of

[49] 50 U.S.C. § 1801(*l*). The term "common carrier" would generally include companies that provide telecommunications services to the public. *See* Kris and Wilson, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 7:6 (Sept. 2019) (citing dictionary definition of "common carrier"). The legislative history of FISA also makes clear that the term "common carrier" refers only to providers operating in the United States. H. REP. NO. 95-1283, at 66.

[50] 50 U.S.C. § 1801(n) (emphasis added).

[51] Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644, 681 (6th Cir. 2007).

[52] *Id*. at 684.

[53] The SCA also includes a "national security letter" provision expressly authorizing the FBI to issue an order compelling the disclosure of certain types of metadata from wire and electronic communication service providers. 18 U.S.C. § 2709. A full discussion of national security letter authorities is beyond the scope of this memorandum. For more information, see CRS Report RL33320, *National Security Letters in Foreign Intelligence Investigations: Legal Background*, by Charles Doyle.

[54] If the government seeks communications metadata from an entity that is not an ECS or an RCS, such as a company that collects, combines, and sells data relating to telephone subscribers but does not provide telephone services or remote computing services, that disclosure would not appear to be regulated by the SCA, and it is not necessary to determine whether Section 2511(2)(f) applies.

disclosures of metadata held by U.S. communications providers, it is unclear whether this would qualify as a foreign intelligence activity *involving a foreign electronic communications system*.[55] Therefore, the discussion below focuses on whether the disclosure qualifies as an acquisition of foreign intelligence information from a foreign or international communication.

As an initial matter, it is important to note that the exempted governmental conduct under Section 2511(2)(f) generally requires some foreign or international nexus, either with respect to the nature of the communication or the nature of the electronic communications system at which a foreign intelligence activity is directed. Therefore, if there is no foreign or international component to the conduct (e.g., if it involves a purely domestic communication in which all parties are in the United States), then the conduct is unlikely to be covered by Section 2511(2)(f). For example, if a person (whether a U.S. citizen or a foreigner) is presently in the United States, then any communications from that individual to another person inside the United States would appear to be fairly characterized as a domestic communication, and therefore not covered as a foreign or international communication, unless the meaning of foreign or international communication includes situations where the communication is routed internationally between two U.S. endpoints. Assuming that is not the case, then the disclosure of metadata about that communication would not appear to be covered by Section 2511(2)(f), and would likely be subject to the SCA's restrictions. However, if the parties to the communication are not all present in the United States, then it would appear to be either a foreign or international communication for purposes of Section 2511(2)(f). If "acquisition" is defined to include receipt of information from a third party (as discussed above), then the disclosure of metadata about that communication appears to be covered under Section 2511(2)(f) if the metadata is foreign intelligence information and the disclosure does not qualify as electronic surveillance under FISA.[56]

When considering whether a disclosure is considered electronic surveillance under FISA, the first question is whether the information was "acqui[red] by an electronic, mechanical, or other surveillance device."[57] This may depend upon whether the collection of metadata by the provider is something that is done in the "ordinary course of business," assuming the definition of "electronic, mechanical, or other device" from ECPA is relevant here.[58] If the metadata is collected in the "ordinary course of business," such as for billing purposes, then arguably it has not been acquired by an electronic, mechanical, or other surveillance device, and would not constitute electronic surveillance under FISA. On the other hand, assuming for the sake of argument that this activity qualifies as an acquisition by electronic, mechanical, or other surveillance device, the next question is whether it involves circumstances protected by a reasonable expectation of privacy in which a warrant would be required for law enforcement purposes. Three of the four categories of electronic surveillance in Section 2511(2)(f) contain this requirement, and as discussed above in the context of the Fourth Amendment, courts do not generally recognize a reasonable expectation of privacy with respect to most kinds of communications metadata, with the notable exception of extended location information.[59]

If extended location metadata is not involved, then the only category of electronic surveillance that could apply is where the metadata concerns a "wire communication to or from a person in the United States, without the consent of any party thereto," and "such acquisition occurs in the United States."[60] For example, continuing the example above, if a U.S. landline telephone provider disclosed metadata about

[55] As noted above, it is possible that a "foreign electronic communications system" could be interpreted to include a domestically located, but foreign owned, system. Insofar as that is a correct reading, the scope of the exception in Section 2511(2)(f) to foreign intelligence activities involving such systems would still be limited by whether or not it constitutes electronic surveillance.

[56] *See supra* note 31 and accompanying text.

[57] 50 U.S.C. § 1801(f)(1)–(4).

[58] 18 U.S.C. § 2510(5).

[59] *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

[60] 50 U.S.C. § 1801(f)(2).

international communications from a user in the United States (whether a citizen or not) to a federal agency such as the NSA, that could fall within the definition of electronic surveillance, again assuming it is an acquisition by electronic, mechanical, or other surveillance device. If the disclosure thus qualifies as electronic surveillance, the disclosure would not be covered by Section 2511(2)(f). However, if it does not qualify as electronic surveillance, either because it is not an acquisition using an electronic, mechanical, or surveillance device, or was not acquired from a wire communication, then Section 2511(2)(f) might apply. Similarly, if "foreign electronic communications system" is understood to include domestically located, but foreign owned, systems, a foreign intelligence activity involving that system could be exempted from Section 2511(2)(f), depending on whether the facts surrounding the activity did or did not constitute electronic surveillance, respectively, and the activity occurred in the United States. However, if neither party to the communication was in the United States at the time it was made, then this definition of electronic surveillance may not be applicable, and the disclosure of metadata concerning that communication to a federal agency might be exempted from the SCA under Section 2511(2)(f) for that reason.

Lastly, it does not appear that the exclusivity clause would affect the analysis above. That clause addresses interception of domestic communications and electronic surveillance under FISA, and domestic communications would likely lack the international or foreign nexus to qualify under the first clause of Section 2511(2)(f). Similarly, if governmental conduct qualifies as electronic surveillance, it is categorically excluded from the exceptions in Section 2511(2)(f), and the exclusivity clause would appear to be redundant.

Conclusion

In summary, the lack of judicial precedent interpreting Section 2511(2)(f) and its related terms may create ambiguities concerning its application to the disclosure of metadata by U.S. communications providers to a federal agency. However, the strongest cases in which it might be applicable are those involving non-location-based metadata concerning communications in which at least one party is outside of the United States, and where such metadata was routinely collected by the provider in the ordinary course of business.