No. COA14-1328 TENTH DISTRICT

NORTH CAROLINA COURT OF APPEALS

****

STATE OF NORTH CAROLINA,	)	
	)	
v.	)	From Wake County
	)	
PAUL GREGORY PERRY,	)	

****

PROPOSED BRIEF OF *AMICI CURIAE*

AMERICAN CIVIL LIBERTIES UNION OF NORTH CAROLINA LEGAL FOUNDATION AND AMERICAN CIVIL LIBERTIES UNION

IN SUPPORT OF DEFENDANT-APPELLANT

****

INDEX

TABLE OF CASES AND AUTHORITIES

Other Authorities

No. COA14-1328 TENTH DISTRICT

NORTH CAROLINA COURT OF APPEALS

****

STATE OF NORTH CAROLINA,	)	
	)	
v.	)	From Wake County
	)	
PAUL GREGORY PERRY.	)	

****

PROPOSED BRIEF OF *AMICI CURIAE*

AMERICAN CIVIL LIBERTIES UNION OF NORTH CAROLINA LEGAL FOUNDATION AND AMERICAN CIVIL LIBERTIES UNION

IN SUPPORT OF DEFENDANT-APPELLANT

****

ARGUMENT

I. REAL TIME CELL PHONE TRACKING REVEALS PRIVATE, INVASIVE, AND INCREASINGLY PRECISE INFORMATION ABOUT INDIVIDUALS' LOCATIONS AND MOVEMENTS.

Because of capabilities built into cell phone networks and handsets in response to federal regulatory requirements, cellular service providers are able to precisely locate cell phones upon law enforcement's request. This capability stems from rules first adopted in 1996 and implemented by 2001, under which the Federal Communications Commission (FCC) required cellular service providers to have "the capability to identify the latitude and longitude of mobile units making

911 calls."[1] The precision and accuracy of this mandated cell phone location capability is increasing. In January 2015, the FCC adopted new rules to increase law enforcement's ability to identify the location of a caller when he or she is indoors,[2] and even to require service providers to develop techniques to reliably determine the altitude of the phone, and thus which floor of a building it is located on.[3]

Although precise location capability was developed initially to assist in responding to 911 calls, service providers now provide the same cell phone location information to law enforcement pursuant to investigative requests. That is, law enforcement can ask a wireless carrier to generate new, precise, real time location data by acquiring information from the target's phone. This can be done "on demand or at periodic intervals," at the direction of law enforcement.[4] In the investigation in this case, law enforcement received updates on the location of Mr. Perry's phone via email every 15 minutes, (T Vol 1 p 21), but location information can also be obtained at shorter intervals.

Importantly, the ability to locate and track a phone in real time has no relationship to whether the phone is actually being used. As long as the telephone is powered on, law enforcement is able to request that the service provider engage

[1] http://transition.fcc.gov/Bureaus/Wireless/Orders/1996/fcc96264.txt.
[2] http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0310/FCC-15-9A1.pdf.
[3] *Id.* at 3-4.
[4] http://www.crypto.com/blog/celltapping/.

its location tracking capabilities; a user cannot disable this functionality.[5] Even enabling the location privacy setting on a smart phone has no effect on the carrier's ability to determine the phone's precise location in real time: while the location privacy setting prevents third-party applications (like the Facebook or Google Maps "apps") from accessing the phone's GPS location information, it does not impact the carrier's ability to do the same.

Service providers can obtain the location of a cell phone upon law enforcement request in at least one of two ways, depending on the structure of the carrier's network. The user's location can be determined either—or both—by using hardware built into the phone ("handset-based" technology) or by a carrier analyzing the phone's interactions with the network's base stations, or "cell sites" ("network-based" technology).[6]

Handset-based technologies use a mobile device's hardware, usually a Global Positioning System (GPS) receiver, which can identify a phone's location to within 10 meters.[7] Newer technology can identify location within 3 meters.[8] Upon law enforcement request, service providers can remotely and covertly

---

[5] http://www.verizonwireless.com/support/e911-compliance-faqs/.
[6] Hearing Before H. Comm. on the Judiciary 113th Cong. 6 (2013) (statement of Matt Blaze, Associate Professor, University of Pennsylvania), http://judiciary.house.gov/_files/hearings/113th/04252013/Blaze%2004252013.pdf.
[7] *Id.* at 7.
[8] http://www.insidegnss.com/node/769.

activate the GPS functionality of a phone and then cause the phone to transmit its GPS coordinates back to the provider.[9]

Network-based technologies use existing cell site infrastructure to identify and track location by silently "pinging" the phone and then triangulating its precise location based on which cell sites receive the reply transmissions.[10] This method can locate any cellular devices connected to a network, regardless of whether they have a GPS chip or not, including tablets and data cards as well as non-GPS enabled phones. As the density of cell sites erected by service providers increases, so does the precision of network-based location capability.[11] In the investigation in this case, law enforcement tracked Mr. Perry's location in real time apparently by "pinging" his phone via this method. (T Vol 1 pp 14, 19, 21, 32-33).

Even greater precision in cell phone location capability results from the growing use of low-power small cells, called "microcells," "picocells," and "femtocells" (collectively, "femtocells"), which provide service to areas as small as ten meters.[12] The number of femtocells nationally now exceeds the number of traditional cell sites.[13] Because the coverage area of femtocells is so small, callers connecting to a carrier's network via femtocells can be located to a high degree of

---

[9] If a phone is unable to calculate its GPS coordinates, the service provider will "fall back" to network-based location calculation.
[10] *Supra* note 6, at 12.
[11] *See* http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey.
[12] https://www.cdt.org/files/file/cell-location-precision.pdf, at 2.
[13] *Id.* at 3.

precision even without triangulation with other cell sites, "sometimes effectively identifying individual floors and rooms within buildings."[14] Femtocells with ranges extending outside of the building in which they are located can also provide cell connections to passersby, providing highly precise information about location and movement on public streets and sidewalks.[15]

The kind of real-time cell phone tracking request at issue in this case is not a rare occurrence: in 2014, AT&T received 13,629 requests for real-time cell phone location information from the government, and many more requests for historical cell phone location records.[16] From 2007 to 2012, Sprint/Nextel received nearly 200,000 court orders for real-time and historical cell phone location information.[17] North Carolina law enforcement agencies make widespread use of cell phone location tracking, with more than 50 state law enforcement agencies stating that they obtain cell phone location data from service providers as of 2011.[18]

---

[14] *Supra* note 6, at 12.

[15] http://www.technologyreview.com/news/514531/qualcomm-proposes-a-cell-phone-network-by-the-people-for-the-people/.

[16] http://about.att.com/content/dam/csr/Transparency%20Reports/ATT_Transparency%20Report_January_2015.pdf.

[17] http://web.archive.org/web/20130415200646/http://markey.house.gov/sites/markey.house.gov/files/documents/Sprint%20Response%20to%20Rep.%20Markey.pdf.

[18] http://www.acluofnc.org/files/legislative/unwarrantedreportfeb2015.pdf.

II. THE STORED COMMUNICATIONS ACT DOES NOT APPLY TO PROSPECTIVE CELL PHONE LOCATION INFORMATION.

The cell phone location information that law enforcement requests usually falls into two types—historical and prospective. Historical location information can be used to retrace previous movements. Prospective location information, the type at issue in this case,[19] can be used to track the phone in real time. Put simply, historical data reveals where a phone *was* while prospective data reveals where a phone *is*.

Here, law enforcement obtained a court order through an application pursuant to 18 U.S.C. § 2701 *et seq*. (2014), otherwise known as the Stored Communications Act ("SCA"). The order authorized the use of "precision location/GPS, E911 locate or Mobile Locate Service if applicable" to track Mr. Perry in real time in the future. (R p 31).[20] Law enforcement did not apply for or receive an actual search warrant supported by probable cause.[21]

---

[19] At the suppression hearing in this case, Officer Mitchell colloquially referred to the cell phone location information as "historical," presumably because it was sent 5-7 minutes after it was obtained by the phone carrier. (T Vol 1 pp 21, 31, 34). As a legal matter, the information was prospective because it did not exist at the time the order was signed and was used to track Mr. Perry in real time. *See United States v. Espudo*, 954 F. Supp. 2d 1029, 1034-35 (S.D. Cal. 2013).

[20] The application also cited N.C. Gen. Stat. §§ 15A-261, 15A-262, and 15A-263. These statutes are limited to pen register and trap and trace devices, which were separately requested in the application but apparently not used in this case.

[21] The fact that the application for the SCA order included the phrase "probable cause" does not convert the application into an application for a warrant, or the order into a warrant, especially because the application used that phrase citing standards that do not at all reflect the Fourth Amendment standard. (R pp 31-32).

The vast majority of courts to consider the issue have concluded that the SCA does not permit the government to obtain this type of prospective cell phone location information, and that prospective location information may only be obtained pursuant to a warrant supported by probable cause. These courts have identified numerous grounds for denying applications for prospective information under the SCA, most notably that the plain language of the statute does not allow it for at least four different reasons.[22] Courts have likewise overwhelmingly rejected government arguments that the combination of the SCA and pen register/trap and trace authorities permits collection of prospective location information. *See, e.g.*, *In re Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816, 827-36 (S.D. Tex. 2006).

In short, the SCA is not the proper vehicle for obtaining prospective cell phone location information. Therefore, courts should require law enforcement to obtain a warrant based on probable cause before engaging in cell phone tracking.

---

[22] For a selection of these cases, *see, e.g.*, *United States v. Espudo*, 954 F. Supp. 2d 1029, 1035 (S.D. Cal. 2013) (citing cases); *In re Application of the United States of America for an Order Relating to Target Phone 2*, 733 F. Supp. 2d 939, 940 n.1 (N.D. Ill. 2009) (same); *In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, and for Geographic Location Information*, 497 F. Supp. 2d 301 (D.P.R. 2007) (same).

III. ACQUISITION OF PROSPECTIVE CELL PHONE LOCATION INFORMATION IS A "SEARCH" UNDER THE FOURTH AMENDMENT AND NORTH CAROLINA CONSTITUTION REQUIRING A WARRANT.

A. Acquisition of Mr. Perry's Prospective Cell Phone Location Information Violates His Reasonable Expectation of Privacy.

The Fourth Amendment[23] does not lose its significance in the face of rapidly advancing technology: "If times have changed reducing everyman's scope to do as he pleases in an urban and industrial world, the changes have made the values served by the Fourth Amendment more, not less, important." *Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971).

In *United States v. Jones*, five Justices agreed that when the government engages in prolonged location tracking, it conducts a search under the Fourth Amendment. 132 S. Ct. 945, 955, 964 (2012). While that case involved law enforcement's installation of a GPS tracking device on a suspect's vehicle and its use to track his location for 28 days, and while the majority relied on a trespass rationale, the majority specified that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* [*v. United States*, 389 U.S. 347 (1967), reasonable-expectation-of-privacy] analysis." *Id.* at 953. Five Justices conducted a *Katz* analysis and concluded that at least

[23] Although the language is markedly different, there is no variance in the rights protected by the Fourth Amendment and North Carolina Constitution Article I, Section 20. *State v. Hendricks*, 43 N.C. App. 245, 251-52, 258 S.E.2d 872, 877-79 (1979).

longer-term location tracking violates reasonable expectations of privacy, regardless of the particular type of technology used to track. *Id.* at 960, 955, 963-964 (Sotomayor, J. & Alito, J. concurring); *see also id.* at 955 (Sotomayor, J.) ("In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention.").

The Supreme Court has also made clear that location tracking that reveals otherwise undiscoverable facts about protected spaces implicates the Fourth Amendment. *See United States v. Karo*, 468 U.S. 705, 714-15 (1984) (holding that use of an electronic device—there, a beeper—to "infer" facts about "location[s] not open to visual surveillance," like whether "a particular article is actually located at a particular time in the private residence," or to later confirm that the article remains on the premises, was just as unreasonable as physically searching the location without a warrant).

These precedents make clear that a warrant is required for the Government to access prospective cell phone location information. First, pursuant to the view of five Justices in *Jones*, at a minimum acquisition of longer-term prospective cell phone location information without a warrant violates the Fourth Amendment. Second, even tracking over a shorter period requires a warrant. The length of time required to implicate the Fourth Amendment is less when it comes to phones as opposed to cars, because individuals are in their cars only for discrete periods of

time and on roads, but they carry their cell phones with them all the time and wherever they go, including to the most private spaces protected by the Fourth Amendment. *See United States v. Davis*, 754 F.3d 1205, 1216 (11th Cir. 2014), *vacated pending rehr'g en banc*, 573 F. App'x 925. Like the tracking in *Karo*, cell phone tracking enables the government to know or infer information about whether the phone is inside a protected location and whether it remains there. People carry their cell phones into many such protected locations, such as the hotel room in this case, where, under *Karo*, the government cannot without a warrant intrude on individuals' reasonable expectations of privacy. *See, e.g., Kyllo v. United States*, 533 U.S. 27, 31 (2001) (home); *See v. City of Seattle*, 387 U.S. 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483, 486–88 (1964) (hotel room). Indeed, that is exactly how the tracking was used in this case, allowing the officers to infer not just that Mr. Perry traveled to a train station and that he went to a hotel, but that Mr. Perry was in one of a certain number of hotel rooms. (T Vol 1 pp 21-23). This danger exists even if cell phone location data is not precise to the exact meter because even imprecise information, when combined with visual surveillance or a known address, can enable law enforcement to "infer" the exact location of a phone. *In re United States for an Order Directing Provider of Elec. Commc'n. Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 311 (3d Cir. 2010).

In the future, such inferences may not even be necessary. The rapid proliferation of femtocells and increasing accuracy of GPS and triangulation data means that for many people, the government will be able to learn their location to the accuracy of a floor or room within their home. And, when requesting prospective location information, the government cannot know if or how the precise data sought implicates a Fourth-Amendment-protected location. As the Supreme Court observed in *Kyllo*, "[n]o police officer would be able to know *in advance* whether his through-the-wall surveillance picks up 'intimate' details—and thus would be unable to know in advance whether it is constitutional." 533 U.S. at 39 (emphasis in original).

To date, the only state supreme courts to address this issue have expressly held that acquisition of prospective cell phone location information is a search requiring a warrant supported by probable cause. *See Tracey v. State*, 152 So.3d 504, 522 (Fla. 2014); *State v. Earls*, 70 A.3d 630, 641 (N.J. 2013); *see also Commonwealth v. Augustine*, 4 N.E.3d 846, 863-64 (Mass. 2014) (addressing historical records).[24] As the Florida Supreme Court explained in *Tracey*, procurement of prospective location information is a search regardless of the length of surveillance or nature of the offense, and a suspect retains a reasonable

[24] The only federal appellate decision directly addressing prospective cell phone location tracking is inapposite because it involved tracking only of a single multi-state car trip on public highways and did not implicate privacy interests in constitutionally protected spaces. *United States v. Skinner*, 690 F.3d 772, 776 (6th Cir. 2012); *see United States v. Powell*, 943 F. Supp. 2d 759, 774 (E.D. Mich. 2013) (distinguishing *Skinner*).

expectation of privacy in this information despite its availability to the phone carrier. 152 So.3d at 522. This Court should reach the same holding.[25]

B. The Third-Party Doctrine Does Not Eliminate Cell Phone Users' Reasonable Expectation of Privacy in their Location.

Under the "third-party doctrine," a person does not have a reasonable expectation of privacy in certain types of information voluntarily conveyed to third parties in certain circumstances. As other courts have held, that principle does not apply in the situation presented here. *In re United States*, 620 F.3d at 318-19; *Tracey*, 152 So.3d at 521-23.

The two main Supreme Court cases addressing the third-party doctrine are instructive but do not reach the surveillance at issue in this case. In *United States v. Miller*, 425 U.S. 435, 440-42 (1976), the Court held that a bank depositor had no expectation of privacy in transaction records that were held by the bank; after analyzing "the nature of the particular documents sought," the Court concluded that the fact that Miller "voluntarily conveyed" the information to the bank and its employees eliminated any expectation of privacy. In *Smith v. Maryland*, 442 U.S. 735, 739-42 (1979), the Court held that the short-term use of a pen register to capture the telephone numbers was not a search under the Fourth Amendment,

[25] Real-time cell tracking is a violation of Article I, Section 20 of the North Carolina Constitution as well as the Fourth Amendment. Therefore, the good faith exception does not apply. *See State v. Carter*, 322 N.C. 709, 710, 370 S.E.2d 553, 554 (1988) (holding that the good faith exception does not exist under the state constitution).

again relying on the fact that when dialing a phone number, the caller "voluntarily convey[s] numerical information to the telephone company." As in *Miller*, the Court also assessed the degree of invasiveness of the surveillance, noting the "pen register's limited capabilities." *Id.*

Under these cases, whether the third-party doctrine applies to cell phone location information thus turns on whether the information is voluntarily conveyed, along with the extent of the privacy interest that people have in it. In a case involving historical records, and where the defendant's location was provided only when he was placing or receiving calls, the Third Circuit explained why cell phone users retain a reasonable expectation of privacy:

> A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all."

In re United States, 620 F.3d at 318–19 (last alteration in original); *accord Davis*, 754 F.3d at 1216–17. This rationale applies with even more force here, where the location information is prospective and collected not when the defendant is making

or receiving calls, but instead continuously without any action or knowledge on his part. *See United States v. Forest*, 355 F.3d 942, 951 (6th Cir. 2004), *vacated on other grounds by Garner v. United States*, 543 U.S. 1100 (2005) (distinguishing *Smith* by noting that the defendant did not voluntarily convey his cell phone location information because a law enforcement agent dialed the defendant's number and caused his phone to send out signals).[26]

In cases of "pinging", the Government's argument can only be that a person gives up any reasonable expectation of privacy simply by owning a phone, despite the fact that he never intentionally or affirmatively discloses his location. Under this logic, people would have no more of a privacy interest in their prospective cell phone location information than they would in trash left on the curb for pickup. That cannot be the case, and no reasonable citizen would think as much.

Furthermore, Congress itself has recognized that citizens have a reasonable expectation of privacy in cell phone location information. *See* 47 U.S.C. §§ 222(c)(1), (h)(1) (prohibiting a phone company's disclosure of "customer proprietary network information ('CPNI')—including "information that relates to the . . . location . . . [of] any customer of a telecommunications carrier . . . that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship"—except "as required by law or with the approval of the

[26] The fact that cell phones include a privacy setting that does not impact a carrier's ability to trace location only gives users a false sense of privacy.

customer"). So has AT&T, the carrier in this very case, whose website informs customers that "regardless of jurisdiction, we require a court order or search warrant for real-time information, stored content such as text and voice messages, and all location requests by law enforcement."[27] The website adds that "[search warrants] are used only in criminal cases, and they are almost always required to obtain real-time location information."[28]

Even if *some* people are now aware from news coverage that service providers can obtain cell phone location information, the reasonable expectation of privacy in the information is not diminished. "[T]he Supreme Court [has] cautioned that where an individual's subjective expectations have been 'conditioned' by influences alien to the well-recognized Fourth Amendment freedoms, a normative inquiry may be necessary to align the individual's expectations with the protections guaranteed in the Fourth Amendment." *Tracey*, 152 So.3d at 513 (quoting *Smith*, 442 U.S. at 740-41).

Finally, the mere fact that a third party has the *ability* to obtain a person's information—like AT&T did here—does not render that information without a reasonable expectation of privacy. *See, e.g., United States v. Warshak*, 631 F.3d 266, 287 (6th Cir. 2010) (recognizing a reasonable expectation of privacy in emails even if a company has a right to access information under the terms of service);

---

[27] *Supra* note 16, at 6-7.
[28] *Id.*

United States v. Paige, 136 F.3d 1012, 1020 n.11 (5th Cir. 1998). The sensitive and private information disclosed by cell phone location data deserves no less protection.

Like the contents of emails, cell phone location information is not a simple business record voluntarily conveyed by the customer. The Supreme Court has cautioned that new technologies should not be allowed to "erode the privacy guaranteed by the Fourth Amendment," *Kyllo*, 533 U.S. at 34, and holding that Mr. Perry had no expectation of privacy simply because he owned a cell phone would do exactly that. As the Florida Supreme Court put it, "[t]he fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone must be rejected." *Tracey*, 152 So.3d at 23 (internal quotation omitted).

CONCLUSION

The Court should hold that the SCA does not allow for real time tracking of cell phones and that, under the Fourth Amendment and the state Constitution, such tracking requires a warrant supported by probable cause.

Respectfully submitted, this the 18th day of March, 2015.

HATCH, LITTLE & BUNN, LLP

Electronically submitted

Laura E. Beaver
N.C. Bar No. 38021
lebeaver@hatchlittlebunn.com

P.O. Box 527
Raleigh, NC 27602
Phone: (919) 856-3979
Fax: (919) 857-3979

Rule 33(b) Certification: I certify that all of the attorneys listed below have authorized me to list their names on this document as if they had personally signed it.

GRAEBE HANNA & SULLIVAN, PLLC

Mark R. Sigmon
N.C. Bar No. 37762
msigmon@ghslawfirm.com
4350 Lassiter at North Hills Ave., Suite 375
Raleigh, NC 27609
Phone: (919) 863-9090
Fax: (919) 863-9095

ACLU OF NORTH CAROLINA LEGAL FOUNDATION

Christopher A. Brook
N.C. Bar No. 33838
cbrook@acluofnc.org
P.O. Box 28004
Raleigh, NC 27611
Phone: (919) 834-3466
Fax: (866) 511-1344

Attorneys for Amici *American Civil Liberties Union of North Carolina Legal Foundation and American Civil Liberties Union*

CERTIFICATE OF COMPLIANCE

This is to certify that the foregoing brief, drafted in proportional type, complies with the requirements of Rule 28(j) of the North Carolina Rules of Appellate Procedure and that the text (including citations and footnotes) contains fewer than 3,750 words (excluding the cover, table of authorities, indices, and certificates of service and compliance), as reported by Microsoft Word.

Electronically submitted
Laura E. Beaver

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the PROPOSED BRIEF OF *AMICI CURIAE* was served on the attorneys of record for parties to this action by first-class mail, addressed as follows:

Elizabeth J. Weese
Assistant Attorney General
N.C. Department of Justice
P.O. Box 629
Raleigh, NC 27602
Attorney for Plaintiff-Appellee

W. Michael Spivey
Post Office Box 1159
Rocky Mount, NC 27802
Attorney for Defendant-Appellant

This the 18th day of March, 2015.

Electronically submitted
Laura E. Beaver

CONTENTS OF APPENDIX

§ 15A-261. Prohibition and exceptions.

(a) In General. – Except as provided in subsection (b) of this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order as provided in this Article.

(b) Exception. – The prohibition of subsection (a) of this section does not apply to the use of a pen register or a trap and trace device by a provider of wire or electronic communication service:

(1) Relating to the operation, maintenance, or testing of a wire or electronic communication service or to the protection of the rights or property of the provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) To record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or

(3) With the consent of the user of that service.

(c) Penalty. – A person who willfully and knowingly violates subsection (a) of this section is guilty of a Class 1 misdemeanor. (1987 (Reg. Sess., 1988), c. 1104, s. 1; 1993, c. 539, s. 297; 1994, Ex. Sess., c. 24, s. 14(c).)

§ 15A-262. Application for order for pen register or trap and trace device.

(a) Application. – A law enforcement officer may make an application for an order or an extension of an order under G.S. 15A-263 authorizing or approving the installation and use of a pen register or a trap and trace device, in writing under oath or affirmation, to a superior court judge.

(b) Contents of application. – An application under subsection (a) of this section shall include:

(1) The identity of the law enforcement officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. (1987 (Reg. Sess., 1988), c. 1104, s. 1.)

§ 15A-263. Issuance of order for pen register or trap and trace device.

(a) In General. – Following application made under G.S. 15A-262, a superior court judge may enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the State if the judge finds:

(1) That there is reasonable suspicion to believe that a felony offense, or a Class A1 or Class 1 misdemeanor offense has been committed;

(2) That there are reasonable grounds to suspect that the person named or described in the affidavit committed the offense, if that person is known and can be named or described; and

(3) That the results of procedures involving pen registers or trap and trace devices will be of material aid in determining whether the person named in the affidavit committed the offense.

(b) Contents of Order. – An order issued under this section:

(1) Shall specify:

a. The identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register or trap and trace device is to be attached;

b. The identity, if known, of the person who is the subject of the criminal investigation;

c. The number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached and, in the case of a trap and trace device, the geographic limits of the trap and trace order; and

d. The offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(2) Shall direct, upon request of the applicant, the furnishing of information, facilities, or technical assistance necessary to accomplish the installation of the pen register or trap and trace device under G.S. 15A-264.

(c) Time Period and Extension.

(1) An order issued under this section shall authorize the installation and use of a pen register or a trap and trace device for a period not to exceed 60 days.

(2) An extension of an order issued under this section may be granted, but only upon an application for an order under G.S. 15A-262 and upon the judicial finding required by subsection (a) of this section. The period of extension shall not exceed 60 days.

(d) Nondisclosure of Existence of Pen Register or a Trap and Trace Device. – An order authorizing or approving the installation and use of a pen register or a trap and trace device shall direct that:

(1) The order be sealed until otherwise ordered by the judge; and

(2) The person owning or leasing the line to which the pen register or a trap and trace device is attached, or who has been ordered by the judge to provide assistance to the applicant, not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any person, unless otherwise ordered by the judge.

The provisions of G.S. 15A-903 and 15A-904 shall apply to this Article. (1987 (Reg. Sess., 1988), c. 1104, s. 1; 1997-80, s. 13.)

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE

PART I - CRIMES

CHAPTER 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

§ 2703. Required disclosure of customer communications or records

(a) Contents of Wire or Electronic Communications in Electronic Storage.— A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Wire or Electronic Communications in a Remote Computing Service.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records Concerning Electronic Communication Service or Remote Computing Service.—

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for Court Order.— A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers 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. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No Cause of Action Against a Provider Disclosing Information Under This Chapter.— No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement To Preserve Evidence.—

(1) In general.— A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.— Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of Officer Not Required.— Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

(Added Pub. L. 99–508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1861; amended Pub. L. 100–690, title VII, §§ 7038, 7039, Nov. 18, 1988, 102 Stat. 4399; Pub. L. 103–322, title XXXIII, § 330003(b), Sept. 13, 1994, 108 Stat. 2140; Pub. L. 103–414, title II, § 207(a), Oct. 25, 1994, 108 Stat. 4292; Pub. L. 104–132, title VIII, § 804, Apr. 24, 1996, 110 Stat. 1305; Pub. L. 104–293, title VI, § 601(b), Oct. 11, 1996, 110 Stat. 3469; Pub. L. 104–294, title VI, § 605(f), Oct. 11, 1996, 110 Stat. 3510; Pub. L. 105–184, § 8, June 23, 1998, 112 Stat. 522; Pub. L. 107–56, title II, §§ 209(2), 210, 212 (b)(1), 220 (a)(1), (b), Oct. 26, 2001, 115 Stat. 283, 285, 291, 292; Pub. L. 107–273, div. B, title IV, § 4005(a)(2), div. C, title I, § 11010, Nov. 2, 2002, 116 Stat. 1812, 1822; Pub. L. 107–296, title II, § 225(h)(1), Nov. 25, 2002, 116 Stat. 2158; Pub. L. 109–162, title XI, § 1171(a)(1), Jan. 5, 2006, 119 Stat. 3123; Pub. L. 111–79, § 2(1), Oct. 19, 2009, 123 Stat. 2086.)

References in Text

The Federal Rules of Criminal Procedure, referred to in subsecs. (a), (b)(1)(A), and (c)(1)(B)(i), are set out in the Appendix to this title.

Amendments

2009—Subsecs. (a), (b)(1)(A), (c)(1)(A). Pub. L. 111–79, which directed substitution of "(or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction" for "by a court with jurisdiction over the offense under investigation or an equivalent State warrant", was executed by making the substitution for "by a court with jurisdiction over the offense under investigation or equivalent State warrant" to reflect the probable intent of Congress.

2006—Subsec. (c)(1)(C). Pub. L. 109–162 struck out "or" at end.

2002—Subsec. (c)(1)(E). Pub. L. 107–273, § 4005(a)(2), realigned margins.

Subsec. (e). Pub. L. 107–296 inserted ", statutory authorization" after "subpoena".

Subsec. (g). Pub. L. 107–273, § 11010, added subsec. (g).

2001—Pub. L. 107–56, § 212(b)(1)(A), substituted "Required disclosure of customer communications or records" for "Requirements for governmental access" in section catchline.

Subsec. (a). Pub. L. 107–56, §§ 209(2)(A), (B), 220 (a)(1), substituted "Contents of Wire or Electronic" for "Contents of Electronic" in heading and "contents of a wire or electronic" for "contents of an electronic" in two places and "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" for "under the Federal Rules of Criminal Procedure" in text.

Subsec. (b). Pub. L. 107–56, § 209(2)(A), substituted "Contents of Wire or Electronic" for "Contents of Electronic" in heading.

Subsec. (b)(1). Pub. L. 107–56, §§ 209(2)(C), 220 (a)(1), substituted "any wire or electronic communication" for "any electronic communication" in introductory provisions and "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" for "under the Federal Rules of Criminal Procedure" in subpar. (A).

Subsec. (b)(2). Pub. L. 107–56, § 209(2)(C), substituted "any wire or electronic communication" for "any electronic communication" in introductory provisions.

Subsec. (c)(1). Pub. L. 107–56, §§ 212(b)(1)(C), 220 (a)(1), designated subpar. (A) and introductory provisions of subpar. (B) as par. (1), substituted "A governmental entity may require a provider of electronic communication service or remote computing service to" for "(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may" and a closing parenthesis for provisions which began with "covered by subsection (a) or (b) of this section) to any person other than a governmental entity." in former subpar. (A) and ended with "(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity", redesignated clauses (i) to (iv) of former subpar. (B) as subpars. (A) to (D), respectively, substituted "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" for "under the Federal Rules of Criminal Procedure" in subpar. (A) and "; or" for period at end of subpar. (D), added subpar. (E), and redesignated former subpar. (C) as par. (2).

Subsec. (c)(2). Pub. L. 107–56, § 210, amended par. (2), as redesignated by section 212 of Pub. L. 107–56, by substituting "entity the—" for "entity the name, address, local and long distance telephone toll billing records,

telephone number or other subscriber number or identity, and length of service of a subscriber" in introductory provisions, inserting subpars. (A) to (F), striking out "and the types of services the subscriber or customer utilized," before "when the governmental entity uses an administrative subpoena", inserting "of a subscriber" at beginning of concluding provisions and designating "to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1)." as remainder of concluding provisions.

Pub. L. 107–56, § 212(b)(1)(C)(iii), (D), redesignated subpar. (C) of par. (1) as par. (2) and temporarily substituted "paragraph (1)" for "subparagraph (B)".

Pub. L. 107–56, § 212(b)(1)(B), redesignated par. (2) as (3).

Subsec. (c)(3). Pub. L. 107–56, § 212(b)(1)(B), redesignated par. (2) as (3).

Subsec. (d). Pub. L. 107–56, § 220(b), struck out "described in section 3127 (2)(A)" after "court of competent jurisdiction".

1998—Subsec. (c)(1)(B)(iv). Pub. L. 105–184 added cl. (iv).

1996—Subsec. (c)(1)(C). Pub. L. 104–293 inserted "local and long distance" after "address,".

Subsec. (d). Pub. L. 104–294 substituted "in section 3127 (2)(A)" for "in section 3126 (2)(A)".

Subsec. (f). Pub. L. 104–132 added subsec. (f).

1994—Subsec. (c)(1)(B). Pub. L. 103–414, § 207(a)(1)(A), redesignated cls. (ii) to (iv) as (i) to (iii), respectively, and struck out former cl. (i) which read as follows: "uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury or trial subpoena;".

Subsec. (c)(1)(C). Pub. L. 103–414, § 207(a)(1)(B), added subpar. (C).

Subsec. (d). Pub. L. 103–414, § 207(a)(2), amended first sentence generally. Prior to amendment, first sentence read as follows: "A court order for disclosure under subsection (b) or (c) of this section may be issued by any court that is a court of competent jurisdiction set forth in section 3127 (2)(A) of this title and shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry."

Pub. L. 103–322 substituted "section 3127 (2)(A)" for "section 3126 (2)(A)".

1988—Subsecs. (b)(1)(B)(i), (c)(1)(B)(i). Pub. L. 100–690, § 7038, inserted "or trial" after "grand jury".

Subsec. (d). Pub. L. 100–690, § 7039, inserted "may be issued by any court that is a court of competent jurisdiction set forth in section 3126 (2)(A) of this title and" before "shall issue".

Effective Date of 2002 Amendment

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

TITLE 47 - TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5 - WIRE OR RADIO COMMUNICATION
SUBCHAPTER II - COMMON CARRIERS
Part I - Common Carrier Regulation

§ 222. Privacy of customer information

(a) In general

Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

(b) Confidentiality of carrier information

A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

(2) Disclosure on request by customers

A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) Aggregate customer information

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.

(d) Exceptions

Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents—

(1) to initiate, render, bill, and collect for telecommunications services;

(2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;

(3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and

(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332 (d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title)—

(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(e) Subscriber list information

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(f) Authority to use location information

For purposes of subsection (c)(1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—

(1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332 (d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title), other than in accordance with subsection (d)(4) of this section; or

(2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

(g) Subscriber listed and unlisted information for emergency services

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service or a provider of IP-enabled voice service (as such term is defined in section 615b of this title) shall provide information described in subsection (i)(3)(A) [1] of this section (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.

(h) Definitions

As used in this section:

(1) Customer proprietary network information

The term "customer proprietary network information" means—

(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

(2) Aggregate information

The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(3) Subscriber list information

The term "subscriber list information" means any information—

(A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

(4) Public safety answering point

The term "public safety answering point" means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

(5) Emergency services

The term "emergency services" means 9–1–1 emergency services and emergency notification services.

(6) Emergency notification services

The term "emergency notification services" means services that notify the public of an emergency.

(7) Emergency support services

The term "emergency support services" means information or data base management services used in support of emergency services.

Footnotes

[1] So in original. Probably should be subsection "(h)(3)(A)".

(June 19, 1934, ch. 652, title II, § 222, as added Pub. L. 104–104, title VII, § 702, Feb. 8, 1996, 110 Stat. 148; amended Pub. L. 106–81, § 5, Oct. 26, 1999, 113 Stat. 1288; Pub. L. 110–283, title III, § 301, July 23, 2008, 122 Stat. 2625.)

Prior Provisions

A prior section 222, act June 19, 1934, ch. 652, title II, § 222, as added Mar. 6, 1943, ch. 10, § 1, 57 Stat. 5; amended July 12, 1960, Pub. L. 86–624, § 36, 74 Stat. 421; Nov. 30, 1974, Pub. L. 93–506, § 2, 88 Stat. 1577; Dec. 24, 1980, Pub. L. 96–590, 94 Stat. 3414; Dec. 29, 1981, Pub. L. 97–130, § 2, 95 Stat. 1687, related to competition among record carriers, prior to repeal by Pub. L. 103–414, title III, § 304(a)(6), Oct. 25, 1994, 108 Stat. 4297.

Amendments

2008—Subsec. (d)(4). Pub. L. 110–283, § 301(1), inserted "or the user of an IP-enabled voice service (as such term is defined in section 615b of this title)" after "section 332 (d) of this title)" in introductory provisions.

Subsec. (f). Pub. L. 110–283, § 301(2), struck out "wireless" before "location" in heading.

Subsec. (f)(1). Pub. L. 110–283, § 301(1), inserted "or the user of an IP-enabled voice service (as such term is defined in section 615b of this title)" after "section 332 (d) of this title)".

Subsec. (g). Pub. L. 110–283, § 301(3), inserted "or a provider of IP-enabled voice service (as such term is defined in section 615b of this title)" after "telephone exchange service".

1999—Subsec. (d)(4). Pub. L. 106–81, § 5(1), added par. (4).

Subsecs. (f), (g). Pub. L. 106–81, § 5(2), added subsecs. (f) and (g). Former subsec. (f) redesignated (h).

Subsec. (h). Pub. L. 106–81, § 5(2)–(4), redesignated subsec. (f) as (h), inserted "location," after "destination," in par. (1)(A), and added pars. (4) to (7).