

Article 16.

Electronic Surveillance.

**§ 15A-286. Definitions.**

As used in this Article, unless the context requires otherwise:

- (1) "Aggrieved person" means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed.
- (2) "Attorney General" means the Attorney General of the State of North Carolina, unless otherwise specified.
- (3) "Aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.
- (4) "Chapter 119 of the United States Code" means Chapter 119 of Part I of Title 18, United States Code, being Public Law 90-351, the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986.
- (5) "Communications common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of Title 47 of the United States Code.
- (6) "Contents" when used with respect to any wire, oral, or electronic communication means and includes any information concerning the substance, purport, or meaning of that communication.
- (7) "Electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than:
  - a. Any telephone or telegraph instrument, equipment, or facility, or any component thereof:
    1. Furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by the subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or
    2. Being used by a provider of wire or electronic communication service in the ordinary course of its business or by an investigative or law enforcement officer in the ordinary course of the officer's duties.
  - b. A hearing aid or similar device being used to correct subnormal hearing to not better than normal.
- (8) "Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce but does not include:
  - a. Any wire or oral communication;
  - b. Any communication made through a tone-only paging device; or
  - c. Any communication from a tracking device (as defined in section 3117 of Title 18 of the United States Code).

- (9) "Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications.
- (10) "Electronic communication system" means any wire, radio, electronic, magnetic, photooptical, or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the storage of such communications.
- (11) "Electronic surveillance" means the interception of wire, oral, or electronic communications as provided by this Article.
- (12) "Electronic storage" means:
  - a. Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
  - b. Any storage of such communication by an electronic communication service for the purposes of backup protection of the communication.
- (13) "Intercept" means the aural or other acquisition of the contents of any wire, oral, or electronic communication through the use of any electronic, mechanical, or other device.
- (14) "Investigative or law enforcement officer" means any officer of the State of North Carolina or any political subdivision thereof, who is empowered by the laws of this State to conduct investigations of or to make arrests for offenses enumerated in G.S. 15A-290, and any attorney authorized by the laws of this State to prosecute or participate in the prosecution of those offenses, including the Attorney General of North Carolina.
- (15) "Judge" means any judge of the trial divisions of the General Court of Justice.
- (16) "Judicial review panel" means a three-judge body, composed of such judges as may be assigned by the Chief Justice of the Supreme Court of North Carolina, which shall review applications for electronic surveillance orders and may issue orders valid throughout the State authorizing such surveillance as provided by this Article, and which shall submit a report of its decision to the Chief Justice.
- (17) "Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but the term does not include any electronic communication.
- (18) "Person" means any employee or agent of the United States or any state or any political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.
- (19) "Readily accessible to the general public" means, with respect to a radio communication, that the communication is not:
  - a. Scrambled or encrypted;
  - b. Transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of the communication;
  - c. Carried on a subcarrier or other signal subsidiary to a radio transmission;
  - d. Transmitted over a communications system provided by a common carrier, unless the communication is a tone-only paging system communication; or

- e. Transmitted on frequencies allocated under Part 25, Subpart D, E, or F or Part 94 of the Rules of the Federal Communications Commission as provided by 18 U.S.C. § 2510(16)(E).
- (20) "User" means any person or entity who:
  - a. Uses an electronic communications service; and
  - b. Is duly authorized by the provider of the service to engage in the use.
- (21) "Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and the term includes any electronic storage of such communication. (1995, c. 407, s. 1; 1997-435, s. 1.)

**§ 15A-287. Interception and disclosure of wire, oral, or electronic communications prohibited.**

- (a) Except as otherwise specifically provided in this Article, a person is guilty of a Class H felony if, without the consent of at least one party to the communication, the person:
  - (1) Willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.
  - (2) Willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:
    - a. The device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communications; or
    - b. The device transmits communications by radio, or interferes with the transmission of such communications.
  - (3) Willfully discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through violation of this Article; or
  - (4) Willfully uses, or endeavors to use, the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this Article.
- (b) It is not unlawful under this Article for any person to:
  - (1) Intercept or access an electronic communication made through an electronic communication system that is configured so that the electronic communication is readily accessible to the general public;
  - (2) Intercept any radio communication which is transmitted:
    - a. For use by the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
    - b. By any governmental, law enforcement, civil defense, private land mobile, or public safety communication system, including police and fire, readily available to the general public;

- c. By a station operating on any authorized band within the bands allocated to the amateur, citizens band, or general mobile radio services; or
  - d. By any marine or aeronautical communication system; or
- (3) Intercept any communication in a manner otherwise allowed by Chapter 119 of the United States Code.

(c) It is not unlawful under this Article for an operator of a switchboard, or an officer, employee, or agent of a provider of electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of employment while engaged in any activity that is a necessary incident to the rendition of his or her service or to the protection of the rights or property of the provider of that service, provided that a provider of wire or electronic communication service may not utilize service observing or random monitoring except for mechanical or service quality control checks.

(d) It is not unlawful under this Article for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of Chapter 5 of Title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(e) Any person who, as a result of the person's official position or employment, has obtained knowledge of the contents of any wire, oral, or electronic communication lawfully intercepted pursuant to an electronic surveillance order or of the pendency or existence of or implementation of an electronic surveillance order who shall knowingly and willfully disclose such information for the purpose of hindering or thwarting any investigation or prosecution relating to the subject matter of the electronic surveillance order, except as is necessary for the proper and lawful performance of the duties of his position or employment or as shall be required or allowed by law, shall be guilty of a Class G felony.

(f) Any person who shall, knowingly or with gross negligence, divulge the existence of or contents of any electronic surveillance order in a way likely to hinder or thwart any investigation or prosecution relating to the subject matter of the electronic surveillance order or anyone who shall, knowingly or with gross negligence, release the contents of any wire, oral, or electronic communication intercepted under an electronic surveillance order, except as is necessary for the proper and lawful performance of the duties of his position or employment or as is required or allowed by law, shall be guilty of a Class 1 misdemeanor.

(g) Any public officer who shall violate subsection (a) or (d) of this section or who shall knowingly violate subsection (e) of this section shall be removed from any public office he may hold and shall thereafter be ineligible to hold any public office, whether elective or appointed. (1995, c. 407, s. 1.)

**§ 15A-288. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited.**

(a) Except as otherwise specifically provided in this Article, a person is guilty of a Class H felony if the person:

- (1) Manufactures, assembles, possesses, purchases, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

- (2) Places in any newspaper, magazine, handbill, or other publication, any advertisement of:
  - a. Any electronic, mechanical, or other device knowing or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or
  - b. Any other electronic, mechanical, or other device where the advertisement promotes the use of the device for the purpose of the surreptitious interception of wire, oral, or electronic communications.

(b) It is not unlawful under this section for the following persons to manufacture, assemble, possess, purchase, or sell any electronic, mechanical, or other device, knowing or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications:

- (1) A communications common carrier or an officer, agent, or employee of, or a person under contract with, a communications common carrier, acting in the normal course of the communications common carrier's business, or
- (2) An officer, agent, or employee of, or a person under contract with, the State, acting in the course of the activities of the State, and with the written authorization of the Attorney General.

(c) An officer, agent, or employee of, or a person whose normal and customary business is to design, manufacture, assemble, advertise and sell electronic, mechanical and other devices primarily useful for the purpose of the surreptitious interceptions of wire, oral, or electronic communications, exclusively for and restricted to State and federal investigative or law enforcement agencies and departments. (1995, c. 407, s. 1.)

**§ 15A-289. Confiscation of wire, oral, or electronic communication interception devices.**

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of G.S. 15A-288 may be seized and forfeited to this State. (1995, c. 407, s. 1.)

**§ 15A-290. Offenses for which orders for electronic surveillance may be granted.**

(a) Orders authorizing or approving the interception of wire, oral, or electronic communications may be granted, subject to the provisions of this Article and Chapter 119 of Title 18 of the United States Code, when the interception does any of the following:

- (1) May provide or has provided evidence of the commission of, or any conspiracy to commit, any of the following:
  - a. Any of the drug-trafficking violations listed in G.S. 90-95(h).
  - b. A continuing criminal enterprise in violation of G.S. 90-95.1.
- (2) May expedite the apprehension of persons indicted for the commission of, or any conspiracy to commit, an offense listed in subdivision (1) of this subsection.

(b) Orders authorizing or approving the interception of wire, oral, or electronic communications may be granted, subject to the provisions of this Article and Chapter 119 of Title 18 of the United States Code, when the interception may provide, or has provided, evidence of any offense that involves the commission of, or any conspiracy to commit, murder, kidnapping, hostage taking, robbery, extortion, bribery, rape, or any sexual offense, or when the interception may expedite the apprehension of persons indicted for the commission of these offenses.

(c) Orders authorizing or approving the interception of wire, oral, or electronic communications may be granted, subject to the provisions of this Article and Chapter 119 of Title 18 of the United States Code, when the interception may provide, or has provided, evidence of any of the following offenses, or any conspiracy to commit these offenses, or when the interception may expedite the apprehension of persons indicted for the commission of these offenses:

- (1) Any felony offense against a minor, including any violation of G.S. 14-27.31 (Sexual activity by a substitute parent or custodian), G.S. 14-27.32 (Sexual activity with a student), G.S. 14-41 (Abduction of children), G.S. 14-43.11 (Human trafficking), G.S. 14-43.12 (Involuntary servitude), G.S. 14-43.13 (Sexual servitude), G.S. 14-190.16 (First degree sexual exploitation of a minor), G.S. 14-190.17 (Second degree sexual exploitation of a minor), G.S. 14-202.1 (Taking indecent liberties with children), G.S. 14-205.2(c) or (d) (Patronizing a prostitute who is a minor or has a mental disability), or G.S. 14-205.3(b) (Promoting prostitution of a minor or a person who has a mental disability).
- (2) Any felony obstruction of a criminal investigation, including any violation of G.S. 14-221.1 (Altering, destroying, or stealing evidence of criminal conduct).
- (3) Any felony offense involving interference with, or harassment or intimidation of, jurors or witnesses, including any violation of G.S. 14-225.2 or G.S. 14-226.
- (4) Any felony offense involving assault or threats against any executive or legislative officer in violation of Article 5A of Chapter 14 of the General Statutes or assault with a firearm or other deadly weapon upon governmental officers or employees in violation of G.S. 14-34.2.
- (5) Any offense involving the manufacture, assembly, possession, storage, transportation, sale, purchase, delivery, or acquisition of weapons of mass death or destruction in violation of G.S. 14-288.8 or the adulteration or misbranding of food, drugs, cosmetics, etc., with the intent to cause serious injury in violation of G.S. 14-34.4.

(d) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized, intercepts wire, electronic, or oral communications relating to offenses other than those specified in the order of authorization or approval, the contents of the communications and evidence derived from the communications may be disclosed or used as provided in G.S. 15A-294(a) and (b). The contents of the communications and any evidence derived from the communications may be used in accordance with G.S. 15A-294(c) when authorized or approved by a judicial review panel where the panel finds, on subsequent application made as soon as practicable, that the contents were otherwise intercepted in accordance with this Article or Chapter 119 of Title 18 of the United States Code.

(e) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this Article or Chapter 119 of Title 18 of the United States Code, shall lose its privileged character. (1995, c. 407, s. 1; 2013-368, s. 6; 2015-181, s. 46; 2018-47, s. 4(k).)

#### **§ 15A-291. Application for electronic surveillance order; judicial review panel.**

(a) The Attorney General or the Attorney General's designee may, pursuant to the provisions of section 2516(2) of Chapter 119 of the United States Code, apply to a judicial review panel for an order authorizing or approving the interception of wire, oral, or electronic

communications by investigative or law enforcement officers having responsibility for the investigation of the offenses as to which the application is made, and for such offenses and causes as are enumerated in G.S. 15A-290. A judicial review panel shall be composed of such judges as may be assigned by the Chief Justice of the Supreme Court of North Carolina or an Associate Justice acting as the Chief Justice's designee, which shall review applications for electronic surveillance orders and may issue orders valid throughout the State authorizing such surveillance as provided by this Article, and which shall submit a report of its decision to the Chief Justice. A judicial review panel may be appointed by the Chief Justice or an Associate Justice acting as the Chief Justice's designee upon the notification of the Attorney General's Office of the intent to apply for an electronic surveillance order.

(b) A judicial review panel is hereby authorized to grant orders valid throughout the State for the interception of wire, oral, or electronic communications. Applications for such orders may be made by the Attorney General or the Attorney General's designee. The Attorney General or the Attorney General's designee in applying for such orders, and a judicial review panel in granting such orders, shall comply with all procedural requirements of section 2518 of Chapter 119 of the United States Code. The Attorney General or the Attorney General's designee may make emergency applications as provided by section 2518 of Chapter 119 of the United States Code. In applying section 2518 the word "judge" in that section shall be construed to refer to the judicial review panel, unless the context otherwise indicates. The judicial review panel may stipulate any special conditions it feels necessary to assure compliance with the terms of this act.

(c) No judge who sits as a member of a judicial review panel shall preside at any trial or proceeding resulting from or in any manner related to information gained pursuant to a lawful electronic surveillance order issued by that panel.

(d) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication must be made in writing upon oath or affirmation to the judicial review panel. Each application must include the following information:

- (1) The identity of the office requesting the application;
- (2) A full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including:
  - a. Details as to the particular offense that has been, or is being committed;
  - b. Except as provided in G.S. 15A-294(i), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted;
  - c. A particular description of the type of communications sought to be intercepted; and
  - d. The identity of the person, if known, committing the offense and whose communications are to be intercepted;
- (3) A full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;
- (4) A statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter must be added;

- (5) A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making adjudication, made to a judicial review panel for authorization to intercept, or for approval of interceptions of wire, oral, or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by that judicial review panel on each such application; and
- (6) Where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(e) Before acting on the application, the judicial review panel may examine on oath the person requesting the application or any other person who may possess pertinent information, but information other than that contained in the affidavit may not be considered by the panel in determining whether probable cause exists for the issuance of the order unless the information is either recorded or contemporaneously summarized in the record or on the face of the order by the panel. (1995, c. 407, s. 1; 1997-435, s. 2; 2005-207, s. 1.)

**§ 15A-292. Request for application for electronic surveillance order.**

(a) The head of any municipal, county, or State law enforcement agency or any district attorney may submit a written request to the Attorney General that the Attorney General apply to a judicial review panel for an electronic surveillance order to be executed within the requesting agency's jurisdiction. The written requests shall be on a form approved by the Attorney General and shall provide sufficient information to form the basis for an application for an electronic surveillance order. The head of a law enforcement agency shall also submit a copy of the request to the district attorney, who shall review the request and forward it to the Attorney General along with any comments he may wish to include. The Attorney General is authorized to review the request and decide whether it is appropriate to submit an application to a judicial review panel for an electronic surveillance order. If a request for an application is deemed inappropriate, the Attorney General shall send a signed, written statement to the person submitting the request, and to the district attorney, summarizing the reasons for failing to make an application. If the Attorney General decides to submit an application to a judicial review panel, he shall so notify the requesting agency head, the district attorney, and the head of the local law enforcement agency which has the primary responsibility for enforcing the criminal laws in the location in which it is anticipated the majority of the surveillance will take place, if not the same as the requesting agency head, unless the Attorney General has probable cause to believe that the latter notifications should substantially jeopardize the success of the surveillance or the investigation in general. If a judicial review panel grants an electronic surveillance order, a copy of such order shall be sent to the requesting agency head and the district attorney, and a summary of the order shall be sent to the head of the local law enforcement agency with primary responsibility for enforcing the criminal laws in the jurisdiction where the majority of the surveillance will take place, if not the same as the requesting agency head, unless the judicial review panel finds probable cause to believe that the latter notifications would substantially jeopardize the success of the surveillance or the investigation.

(b) This Article does not limit the authority of the Attorney General to apply for electronic surveillance orders independent of, or contrary to, the requests of law enforcement agency heads, nor does it limit the discretion of the Attorney General in determining whether an application is appropriate under any given circumstances.



(c) The Chief Justice of the North Carolina Supreme Court shall receive a report concerning each decision of a judicial review panel. (1995, c. 407, s. 1.)

**§ 15A-293. Issuance of order for electronic surveillance; procedures for implementation.**

(a) Upon application by the Attorney General pursuant to the procedures in G.S. 15A-291, a judicial review panel may enter an ex parte order, as requested or as modified, authorizing the interception of wire, oral, or electronic communications, if the panel determines on the basis of the facts submitted by the applicant that:

- (1) There is probable cause for belief that an individual is committing, has committed, or is about to commit an offense set out in G.S. 15A-290;
- (2) There is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
- (3) Normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; and
- (4) Except as provided in G.S. 15A-294(i), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by the individual described in subdivision (1) of this subsection.

(b) Each order authorizing the interception of any wire, oral, or electronic communications must specify:

- (1) The identity of the person, if known, whose communications are to be intercepted;
- (2) The nature and location of the communications facilities as to which, or the place where, authority to intercept is granted, and the means by which such interceptions may be made;
- (3) A particular description of the type of communication sought to be intercepted and a statement of the particular offense to which it relates;
- (4) The identity of the agency authorized to intercept the communications and of the person requesting the application; and
- (5) The period of time during which such interception is authorized, including a statement as to whether or not the interception automatically terminates when the described communication has been first obtained.

(c) No order entered under this Article may authorize the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than 30 days. Such 30-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or 10 days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with G.S. 15A-291 and the panel making the findings required by subsection (a) of this section. The period of extension shall be no longer than the panel determines to be necessary to achieve the purpose for which it was granted and in no event for longer than 30 days. Every order and extension thereof must contain a provision that the authorization to intercept be executed as soon as practicable, be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this Article, and terminate upon attainment of the authorized objective, or in any event in 30 days, as is

appropriate. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after the interception. An interception under this Article may be conducted in whole or in part by State or federal government personnel, or by an individual operating under a contract with the State or federal government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(d) Whenever an order authorizing interception is entered pursuant to this Article, the order may require reports to be made to the issuing judicial review panel showing that progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports must be made at such intervals as the panel may require.

- (1) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this Article must be recorded on tape, wire, or electronic or other comparable device. The recording of the contents of any wire, electronic, or oral communication under this subsection must be done in such way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, the recordings must be made available to the judicial review panel and sealed under its direction. Custody of the recordings is wherever the panel orders. They may not be destroyed except upon an order of the issuing panel and in any event must be kept for 10 years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of G.S. 15A-294(a) and (b) for investigations. The contents of any wire, oral, or electronic communication or evidence derived therefrom may not be disclosed or used under G.S. 15A-294(c) unless they have been kept sealed.
- (2) Applications made and orders granted under this Article must be sealed by the panel. Custody of the applications and orders may be disclosed only upon a showing of good cause before the issuing panel and may not be destroyed except on its order and in any event must be kept for 10 years.
- (3) Any violation of the provisions of this subsection may be punished as for contempt.

(e) The State Bureau of Investigation shall own or control and may operate any equipment used to implement electronic surveillance orders issued by a judicial review panel and may operate or use, in implementing any electronic surveillance order, electronic surveillance equipment in which a local government or any of its agencies has a property interest.

(f) The Attorney General shall establish procedures for the use of electronic surveillance equipment in assisting local law enforcement agencies implementing electronic surveillance orders. The Attorney General shall supervise such assistance given to local law enforcement agencies and is authorized to conduct statewide training sessions for investigative and law enforcement officers regarding this Article. (1995, c. 407, s. 1; 1997-435, s. 2.1; 2005-207, ss. 2, 3.)

#### **§ 15A-294. Authorization for disclosure and use of intercepted wire, oral, or electronic communications.**

(a) Any investigative or law enforcement officer who, by any means authorized by this Article or Chapter 119 of the United States Code, has obtained knowledge of the contents of any

wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(b) Any investigative or law enforcement officer, who by any means authorized by this Article or Chapter 119 of the United States Code, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may use such contents to the extent such use is appropriate to the proper performance of the officers' official duties.

(c) Any person who has received, by any means authorized by this Article or Chapter 119 of the United States Code, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom, intercepted in accordance with the provisions of this Article, may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding in any court or before any grand jury in this State, or in any court of the United States or of any state, or in any federal or state grand jury proceeding.

(d) Within a reasonable time, but no later than 90 days after the filing of an application for an order or the termination of the period of an order or the extensions thereof, the issuing judicial review panel must cause to be served on the persons named in the order or the application and such other parties as the panel in its discretion may determine, an inventory that includes notice of:

- (1) The fact of the entry of the order or the application;
- (2) The date of the entry and the period of the authorized interception; and
- (3) The fact that during the period wire, oral, or electronic communications were or were not intercepted.

(d1) The notification required pursuant to G.S. 15A-294(d) may be delayed if the judicial review panel has probable cause to believe that notification would substantially jeopardize the success of an electronic surveillance or a criminal investigation. Delay of notification shall be only by order of the judicial review panel. The period of delay shall be designated by the judicial review panel and may be extended from time to time until the jeopardy to the electronic surveillance or the criminal investigation dissipates.

(e) The issuing judicial review panel, upon the filing of a motion, may in its discretion, make available to such person or his counsel for inspection, such portions of the intercepted communications, applications, and orders as the panel determines to be required by law or in the interest of justice.

(f) The contents of any intercepted wire, oral, or electronic communication, or evidence derived therefrom, may not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in any court of this State unless each party, not less than 20 working days before the trial, hearing, or other proceeding, has been furnished with a copy of the order and accompanying application, under which the interception was authorized.

(g) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of this State, or a political subdivision thereof, may move to suppress the contents of any intercepted wire, oral, or electronic communication, or evidence derived therefrom, on the grounds that:

- (1) The communication was unlawfully intercepted;
- (2) The order of authorization under which it was intercepted is insufficient on its face; or
- (3) The interception was not made in conformity with the order of authorization.

Such motion must be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of this motion. If the motion is granted, the contents of the intercepted wire, oral, or electronic communication, or evidence derived therefrom, must be treated as having been obtained in violation of this Article.

(h) In addition to any other right to appeal, the State may appeal:

- (1) From an order granting a motion to suppress made under subdivision (1) of this subsection, if the district attorney certifies to the judge granting the motion that the appeal is not taken for purposes of delay. The appeal must be taken within 30 days after the date the order of suppression was entered and must be prosecuted as are other interlocutory appeals; or
- (2) From an order denying an application for an order of authorization, and the appeal may be made ex parte and must be considered in camera and in preference to all other pending appeals.

(i) The requirements of G.S. 15A-293(b)(2) and G.S. 15A-293(a)(4) relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if:

- (1) In the case of an application with respect to the interception of an oral communication:
  - a. The application is by a State investigative or law enforcement officer and is approved by the Attorney General or his designee;
  - b. The application contains a full and complete statement as to why the specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and
  - c. The judicial review panel finds that the specification is not practical.
- (2) In the case of an application with respect to a wire or electronic communication:
  - a. The application is by a State investigative or law enforcement officer and is approved by the Attorney General or his designee;
  - b. The application identifies the person believed to be committing the offense and whose communications are to be intercepted, and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility;
  - c. The judicial review panel finds that the showing has been adequately made; and
  - d. The order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which the communication will be or was transmitted.

(j) An interception of a communication under an order with respect to which the requirements of G.S. 15A-293(b)(2) and G.S. 15A-293(a)(4) do not apply by reason of subdivision (i)(1) of this section shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order. A provider of wire or electronic communications service that has received an order as provided for in subdivision (i)(2) of this section may move the court to modify or quash the order on the grounds that its assistance with respect to the interception cannot be performed in a timely or reasonable fashion. The court, upon

notice to the government, shall decide such a motion expeditiously. (1995, c. 407, s. 1; 1997-435, s. 3; 2005-207, s. 4.)

**§ 15A-295. Reports concerning intercepted wire, oral, or electronic communications.**

In January of each year, the Attorney General of this State must report to the Administrative Office of the United States Court the information required to be filed by section 2519 of Title 18 of the United States Code, as heretofore or hereafter amended, and file a copy of the report with the Administrative Office of the Courts of North Carolina. (1995, c. 407, s. 1.)

**§ 15A-296. Recovery of civil damages authorized.**

(a) Any person whose wire, oral, or electronic communication is intercepted, disclosed, or used in violation of this Article, has a civil cause of action against any person who intercepts, discloses, uses, or procures any other person to intercept, disclose, or use such communications, and is entitled to recover from any other person:

- (1) Actual damages, but not less than liquidated damages, computed at the rate of one hundred dollars (\$100.00) a day for each day of violation or one thousand dollars (\$1,000), whichever is higher;
- (2) Punitive damages; and
- (3) A reasonable attorneys' fee and other litigation costs reasonably incurred.

(b) Good faith reliance on a court order or on a representation made by the Attorney General or a district attorney is a complete defense to any civil or criminal action brought under this Article. (1995, c. 407, s. 1.)

**§ 15A-297. Conformity to provisions of federal law.**

It is the intent of this Article to conform the requirements of all interceptions of wire, oral, or electronic communications conducted by investigative or law enforcement officers in this State to provisions of Chapter 119 of the United States Code, except where the context indicates a purpose to provide safeguards even more protective of individual privacy and constitutional rights. (1995, c. 407, s. 1.)

**§ 15A-298. Subpoena authority.**

The Director of the State Bureau of Investigation or the Director's designee may issue an administrative subpoena to a communications common carrier or an electronic communications service to compel production of business records if the records:

- (1) Disclose information concerning local or long-distance toll records or subscriber information; and
- (2) Are material to an active criminal investigation being conducted by the State Bureau of Investigation. (1995, c. 407, s. 1; 1997-435, s. 4; 2014-100, s. 17.1(ee); 2015-276, s. 4.)