Tenn. Code Ann. § 39-13-601

Current through Chapter 900, with the exception of Chapter 688 secs 79, 80, and 83, of the 2024 Regular Session. The commission may make editorial changes to this version and may relocate or redesignate text. Those changes will appear on Lexis Advance after the publication of the certified volumes and supplements. Pursuant to TCA sections 1-1-110, 1-1-111, and 1-2-114, the Tennessee Code Commission certifies the final, official version of the Tennessee Code. Until the annual issuance of the certified volumes and supplements, references to the updates made by the most recent legislative session should be to the Public Chapter and not TCA.

TN - Tennessee Code Annotated > Title 39 Criminal Offenses > Chapter 13 Offenses Against Person > Part 6 Invasion of Privacy

39-13-601. Wiretapping and electronic surveillance — Prohibited acts — Exceptions.

(a)

- (1) Except as otherwise specifically provided in §§ 39-13-601 39-13-603 and title 40, chapter 6, part 3, a person commits an offense who:
 - (A) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
 - **(B)** Intentionally 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:
 - (i) The device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
 - (ii) The device transmits communications by radio, or interferes with the transmission of the communication;
 - **(C)** Intentionally 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 the interception of a wire, oral, or electronic communication in violation of this subsection (a); or
 - **(D)** Intentionally uses, or endeavors to use, the contents of any wire, oral or electronic communication, knowing or having reason to know, that the information was obtained through the interception of a wire, oral or electronic communication in violation of this subsection (a).
- (2) A violation of subdivision (a)(1) shall be punished as provided in § 39-13-602 and shall be subject to suit as provided in § 39-13-603.

- (1) It is lawful under §§ 39-13-601 39-13-603 and title 40, chapter 6, part 3 for an officer, employee, or agent of a provider of wire or electronic communications service, or a telecommunications company, whose facilities are used in the transmission of a wire communication, to intercept, disclose or use that communication in the normal course of employment while engaged in any activity that is necessary to the rendition of service or to the protection of the rights or property of the provider of that service. Nothing in §§ 39-13-601 39-13-603 and title 40, chapter 6, part 3 shall be construed to prohibit a telecommunications or other company from engaging in service observing for the purpose of maintaining service quality standards for the benefit of consumers.
- (2) Notwithstanding any other law, providers of wire or electronic communications service, their officers, employees, or agents, landlords, custodians, or other persons are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications, if the provider, its officers, employees, or agents, landlord, custodian or other specified person has been provided with a court order signed by the authorizing judge of competent jurisdiction that:
 - (A) Directs the assistance;
 - **(B)** Sets forth a period of time during which the provision of the information, facilities, or technical assistance is authorized; and
 - (C) Specifies the information, facilities, or technical assistance required.
- (3) No provider of wire or electronic communications service, officer, employee, or agent thereof, or landlord, custodian or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order, except as may otherwise be required by legal process, and then only after prior notification to the attorney general and reporter or to the district attorney general or any political subdivision of a district, as may be appropriate. Any such disclosure shall render the person liable for the civil damages provided for in § 39-13-603. No cause of action shall lie in any court against any provider of wire or electronic communications service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order under §§ 39-13-601 39-13-603 and title 40, chapter 6, part 3.
- (4) It is lawful under §§ 39-13-601 39-13-603 and title 40, chapter 6, part 3 for a person acting under the color of law to intercept a wire, oral or electronic communication, where the person is a party to the communication or one of the parties to the communication has given prior consent to such interception.
- (5) It is lawful under §§ 39-13-601 39-13-603 and title 40, chapter 6, part 3 for a person not acting under color of law to intercept a wire, oral, or electronic communication, where the person is a party to the communication or where one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of this state.
- (6) It is unlawful to intercept any wire, oral, or electronic communication for the purpose of committing a criminal act.
- (7) It is lawful, unless otherwise prohibited by state or federal law, for any person:

- (A) To 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;
- **(B)** To intercept any radio communication that is transmitted by:
 - (i) Any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
 - (ii) Any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;
 - (iii) Any station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
 - (iv) Any marine or aeronautical communications system;
- **(C)** To intercept any wire or electronic communication, the transmission of which is causing harmful interference with any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or
- **(D)** For other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(c)

- (1) Except as provided in subdivision (c)(2), a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication, other than one to such person or entity, or an agent thereof, while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.
- (2) A person or entity providing electronic communication service to the public may divulge the contents of any such communication:
 - (A) As otherwise authorized in subdivisions (b)(1)-(3) or \S 40-6-306;
 - **(B)** With the lawful consent of the originator or any addressee or intended recipient of such communication;
 - **(C)** To a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or
 - **(D)** That were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if the divulgence is made to a law enforcement agency.
- (d) Notwithstanding any provision of this part to the contrary, this section shall not apply to a person who installs software on a computer the person owns if such software is intended solely to monitor and record the use of the internet by a minor child of whom such person is a parent or legal guardian.

History

Acts 1994, ch. 964, \S 4; 2011, ch. 460, \S 1.

TENNESSEE CODE ANNOTATED

Copyright © 2024 by The State of Tennessee All rights reserved

End of Document