West's Hawai'i Revised Statutes Annotated
Division 5. Crimes and Criminal Proceedings
Title 38. Procedural and Supplementary Provisions
Chapter 803. Arrests, Searches, Search Warrants (Refs & Annos)
Part IV. Electronic Eavesdropping

HRS § 803-42

§ 803-42. Interception, access, and disclosure of wire, oral, or electronic communications, use of pen register, trap and trace device, and mobile tracking device prohibited

Currentness

(a) Except as otherwise specifically provided in this part, any person who:

(1) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(2) 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 wire, oral, or electronic communication when:

(A) Such a device is affixed to, or otherwise transmits a signal through, a wire, cable, or other similar connection used in wire communication; or

(B) Such a device transmits communications by radio, or interferes with the transmission of such communication;

(3) 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 part;

(4) 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 part;

(5)(A) Intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(B) Intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage;

(6) Intentionally discloses, or attempts to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by subsection (b)(1), (2), or (3), or section 803-44 or 803-46; and

(A) Either:

(i) Knowing or having reason to know that the information was obtained through the interception of the communication in connection with a criminal investigation; or

(ii) Having obtained or received the information in connection with a criminal investigation; and

(B) With the intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation[;]

(7) Intentionally installs or uses a pen register or a trap and trace device without first obtaining a court order; or

(8) Intentionally installs or uses a mobile tracking device without first obtaining a search warrant or other order authorizing the installation and use of such device, unless the device is installed by or with consent of the owner of the property on which the device is installed;

shall be guilty of a class C felony.

(b)(1) It shall not be unlawful under this part for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication services, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of the officer's, employee's, or agent's employment while engaged in any activity that is either a necessary incident to the rendition of the officer's, employee's, or agent's service or to the protection of the rights or property of the provider of that service; provided that providers of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(2) It shall not be unlawful under this part for an officer, employee, or agent of the Federal Communications Commission, in the normal course of the officer's, employee's, or agent's employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of title 47, chapter 5, 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.

(3)(A) It shall not be unlawful under this part for a person not acting under color of law to intercept a wire, oral, or electronic communication when the person is a party to the communication or when 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 the United States or of this State.

(B) It shall not be unlawful for a person acting under color of law to install in any private place, without consent of the person or persons entitled to privacy therein, any device for recording, amplifying, or broadcasting sounds or events

in that place, or use of any such unauthorized installation, or install or use outside a private place any such device to intercept sounds originating in that place which would not ordinarily be audible or comprehensible outside.

(4) It shall not be unlawful under this part for a person acting under color of law to intercept a wire, oral, or electronic communication, when the person is a party to the communication or one of the parties to the communication has given prior consent to the interception.

(5) It shall not be unlawful under this part for any person to intercept a wire, oral, or electronic communication, or to disclose or use the contents of an intercepted communication, when such interception is pursuant to a valid court order under this chapter or otherwise authorized by law; provided that a communications provider with knowledge of an interception of communications accomplished through the use of the communications provider's facilities shall report the fact and duration of the interception to the administrative director of the courts of this State.

(6) Notwithstanding any other law to the contrary, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept or access wire, oral, or electronic communications, to conduct electronic surveillance, or to install a pen register or trap and trace device if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with:

(A) A court order directing such assistance signed by the designated judge; or

(B) A certification in writing from the Attorney General of the United States, the Deputy Attorney General of the United States, the Associate Attorney General of the United States, the attorney general of the State of Hawaii, or the prosecuting attorney for each county that no warrant or court order is required by law, that all statutory requirements have been met, and that the specific assistance is required, setting forth the period of time during which the providing of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required.

No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any access, interception, or surveillance or the device used to accomplish the interception or surveillance for which the person has been furnished a court order or certification under this part, except as may otherwise be required by legal process and then only after prior notification to the party that provided the court order or certification.

No cause of action shall lie in any court against any provider of wire or electronic communication 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 or certification under this part.

(7) It shall not be unlawful under this part for any person:

(A) To intercept or access an electronic communication made through an electronic communication system configured so that the electronic communication is readily accessible to the general public.

(B) To intercept any radio communication that is transmitted:

(i) By any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(ii) By any governmental, law enforcement, emergency management, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;

(iii) By a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or

(iv) By any marine or aeronautical communications system.

(C) To engage in any conduct that:

(i) Is prohibited by section 633 of the Communications Act of 1934 (47 U.S.C. § 553); or

(ii) Is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act (47 U.S.C. § 605).

(D) To intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment to the extent necessary to identify the source of the interference.

(E) For other users of the same frequency to intercept any radio communication made through a system that uses frequencies monitored by individuals engaged in the providing or the use of the system, if the communication is not scrambled or encrypted.

(8) It shall not be unlawful under this part:

(A) To use a pen register or a trap and trace device as specified in this part.

(B) For a provider of electronic communication service 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 or electronic communication, or a user of that service, from the fraudulent, unlawful, or abusive use of such service.

(C) For a provider of electronic or wire communication service to use a pen register or a trap and trace device for purposes relating to the operation, maintenance, and testing of the 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.

(D) To use a pen register or a trap and trace device where consent of the user of the service has been obtained.

(9) Good faith reliance upon a court order shall be a complete defense to any criminal prosecution for illegal interception, disclosure, or use.

(10) Except as provided in this section, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than a communication to the 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 the communication or an agent of the addressee or intended recipient.

(11) A person or entity providing electronic communication service to the public may divulge the contents of any such communication:

(A) As otherwise authorized by a court order or under this part;

(B) With the lawful consent of the originator, addressee, or intended recipient of the communication;

(C) To a person employed or authorized, or whose facilities are used, to forward the communication to its destination;

(D) That was inadvertently obtained by the service provider and that appears to pertain to the commission of a crime, if divulged to a law enforcement agency; or

(E) To a law enforcement agency, public safety agency, or public safety answering point if the provider, in good faith, believes that an emergency involving danger of death or serious bodily injury to any person requires disclosure without delay of communications relating to the emergency, and is provided with a certification in writing from the governmental entity that provides the facts and circumstances establishing the existence of the emergency, that the specific disclosure is required, and sets forth the period of time during which the disclosure of the information is authorized and specifies the information required.

No cause of action shall lie in any court against any provider of electronic communication service, its officers, employees, or agents, custodian, or other specified person for disclosing information in accordance with the terms of a certification under this part.

Credits

Laws 1978, ch. 218, § 2; Laws 1984, ch. 90, § 1; Laws 1986, ch. 303, § 2; Laws 1989, ch. 164, § 4; Laws 2006, ch. 200, § 4; Laws 2012, ch. 94, § 1, eff. April 30, 2012; Laws 2014, ch. 111, § 28, eff. July 1, 2014.

Notes of Decisions (29)

H R S § 803-42, HI ST § 803-42

Current through the 2025 Regular Session, pending text revision by the revisor of statutes.

End of Document