ACT 164

H.B. NO. 1716

A Bill for an Act Relating to Interception of Communications.

Be It Enacted by the Legislature of the State of Hawaii:

SECTION 1. Chapter 803, Hawaii Revised Statutes, is amended by adding five new sections to be appropriately designated and to read as follows:

"§803- Disclosure of contents of communication while in electronic storage.

(a) (1) A person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) A person or entity providing remote computing services to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried 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 transmissions from) a subscriber or customer of such service; and

(B) Solely for the purpose of providing storage and 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.

(b) A person or entity may divulge the contents of a communication:

(1) To an addressee, intended recipient, or the addressee's or intended recipient's agent, of such communication;

(2) As otherwise authorized by a court order or search warrant;

(3) With the lawful consent of the originator, addressee, or intended recipient of such communication, or the subscriber in the case of a remote computing service;

(4) To a person employed or authorized or whose facilities are used to forward such communication to its destination.

(5) As may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

(6) To a law enforcement agency, if such contents:

(A) Were inadvertently obtained by the service provider; and

(B) Appear to pertain to the commission of a crime.

§803- **Requirements for governmental access.** (a) A governmental entity may require disclosure of the contents of an electronic communication that has been in electronic storage for one hundred eighty days, or less, from the provider of the electronic communication service where storage has taken place, only by means of a search warrant. A governmental entity may require disclosure of the contents of an electronic communication which has been in electronic storage for more than one hundred eighty days by the means available under subsection (b) of this section.

(b) A governmental entity may require a provider of remote computing services to disclose the contents of any electronic communication to which this subsection is made applicable by subsection (c) of this section:

(1) Without notice to the subscriber or customer, if a search warrant has been obtained; or

(2) With prior notice to the subscriber or customer, if a court order for disclosure under subsection (d) of this section has been obtained; except that delayed notice may be authorized by the order.

(c) Subsection (b) of this section is applicable to any electronic communication held or maintained on a remote computing service:

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

(2) 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 any purpose other than storage or computer processing.

(d) (1) A provider of electronic communication or remote computing services may disclose a record or other information pertaining to a subscriber or customer of such service (other than the contents of any electronic communication) to any person other than a governmental entity.

(2) A provider of electronic communication or remote computing services shall disclose a record or other information pertaining to a subscriber or customer of such service (other than the contents of an electronic communication) to a governmental entity only when:

(A) Presented with a grand jury subpoena;

(B) Presented with a search warrant;

(C) Presented with a court order for such disclosure; or

(D) The consent of the subscriber or customer to such disclosure has been obtained.

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

(e) A court order for disclosure under subsection (b) or (c) or this section shall issue only if the governmental entity demonstrates probable cause that the contents of a wire or electronic communication, or records or other information sought, constitute or relate to the fruits, implements, or existence of a crime or are relevant to a legitimate law enforcement inquiry. An order may be quashed or modified if, upon a motion promptly made, the service provider shows that compliance would be unduly burdensome because of the voluminous nature of the information or records requested, or some other stated reason establishing such a hardship.

(f) 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, or subpoena.

§803- Backup preservation. (a) A governmental entity may include in its court order a requirement that the service provider create a backup copy of the contents of the electronic communication without notifying the subscriber or customer. The service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such a backup copy has been made. Such backup copy shall be created within two business days after receipt of a subpoena or court order by the service provider.

(b) The governmental entity must give notice to the subscriber or customer within three days of receiving confirmation that a backup record has been made, unless notice is delayed pursuant to the procedures herein.

(c) The service provider shall not destroy such backup copy until the later of:

(1) The delivery of the information; or

(2) The resolution of any proceedings, including any appeal therefrom, concerning a court order.

(d) The service provider shall release such backup copy to the requesting governmental entity no sooner than fourteen days after the governmental entity's notice to the subscriber or customer, if such service provider:

(1) Has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(2) Has not initiated proceedings to challenge the governmental entity's request.

(e) Within fourteen days after notice by the governmental entity to the subscriber or customer under subsection (b) of this section, the subscriber or customer may file a motion to vacate such court order with written notice and a copy of the motion being served on both the governmental entity and the service provider. The motion to vacate a court order shall be filed with the circuit court judge designated by the chief justice of the Hawaii supreme court. Such motion or application shall contain an affidavit or sworn statement:

(1) Stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications are sought; and

(2) Setting forth the applicant's reasons for believing that the records sought does not constitute probable cause or there has not been substantial compliance with some aspect of the provisions of this part.

(f) Upon receiving a copy of the motion from the subscriber or customer, the governmental agency shall file a sworn response to the court to which the motion is assigned. The response shall be filed within fourteen days. The response may ask the court for an in camera review, but must state reasons justifying such a review. If the court is unable to rule solely on the motion or application and response submitted, the court may conduct such additional proceedings as it deems appropriate. A ruling shall be made as soon as practicable after the filing of the governmental entity's response.

(g) If the court finds that the applicant is not the subscriber or customer whose communications are sought, or that there is reason to believe that the law enforcement inquiry is legitimate and the justification for the communications sought is supported by probable cause, the application or motion shall be denied, and the court shall order the release of the backup copy to the government entity. A court order denying a motion or application shall not be deemed a final order, and no interlocutory appeal may be taken therefrom by the customer. If the court finds that the applicant is a proper subscriber or customer and the justification for the communication sought is not supported by probable cause or that there has not been substantial compliance with the provisions of this part, it shall order vacation of the order previously issued.

§803- Delay of notification. (a) A governmental entity may as part of a request for a court order include a provision that notification be delayed for a period not exceeding ninety days if the court determines that notification of the existence of the court order may have an adverse result.

(b) An adverse result for the purpose of subsection (a) of this section is:

(1) Endangering the life or physical safety of an individual;

(2) Flight from prosecution;

(3) Destruction of or tampering with evidence;

(4) Intimidation of a potential witness; or

(5) Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(c) Extensions of delays in notification may be granted up to ninety days per application to a court. Each application for an extension must comply with subsection (e) of this section.

(d) Upon expiration of the period of delay of notification, the governmental entity shall serve upon, or deliver by registered mail to, the customer or subscriber a copy of the process or request together with notice that:

(1) States with reasonable specificity the nature of the law enforcement inquiry; and
(2) Informs such customer or subscriber:
(A) That information maintained for such customer or subscriber by the service provider or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;
(B) That notification of such customer or subscriber was delayed;
(C) What governmental entity or court made the certification or determination; and
(D) Which provision of this part allowed such delay.

(e) A governmental entity may apply to the circuit court designated by the chief justice of the Hawaii supreme court or any other circuit judge or district court judge, if a circuit court judge has not yet been designated by the chief justice of the Hawaii supreme court, or is otherwise unavailable, for an order commanding a provider of an electronic communication service or remote computing service to whom a search warrant, or court order is directed, not to notify any other person of the existence of the search warrant, or court order for such period as the court deems appropriate not to exceed ninety days. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the search warrant, or court order will result in:
(1) Endangering the life or physical safety of an individual;
(2) Flight from prosecution;
(3) Destruction of or tampering with evidence;
(4) Intimidation of a potential witness; or
(5) Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§803- Cost reimbursement. A government entity obtaining the contents of communications, records, or other information shall reimburse any person or entity reasonable fees for providing or assembling such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service which was occasioned by the governmental needs."

SECTION 2. Chapter 803, Hawaii Revised Statutes, is amended by adding three new sections to be appropriately designated and to read as follows:

"§803- Application for a pen register or a trap and trace device. (a) The attorney general of this State or the prosecuting attorney for each county, or a subordinate designated to act in either's absence or incapacity, may apply in writing under oath or equivalent affirmation to a circuit court judge designated by the chief justice of the Hawaii supreme court or any other circuit court judge or district court judge, if a circuit court judge has not been designated by the chief justice of the Hawaii supreme court, or is otherwise unavailable, for an order or extension of an order to authorize the installation and use of a pen register or a trap and trace device.

(b) The application shall include:
(1) The identity of the official making the application and the law enforcement agency conducting the investigation; and
(2) The facts and circumstances relied upon by the applicant to conclude that there is probable cause to believe that information will be obtained through the installation and use of a pen register or trap and trace device which will constitute the fruits, instrumentalities, or evidence of a crime covered under this part.

§803- Issuance of an order for a pen register or a trap and trace device. (a) Upon application for an order authorizing the installation and use of a pen register or a trap and trace device, the reviewing judge shall satisfy itself that there are sufficient facts and circumstances contained within the application that there is probable cause to believe that information will be obtained through the installation and use of a pen register or a trap and trace device which will constitute the fruits, instrumentalities, or evidence of a crime or is relevant to an ongoing criminal investigation.

(b) If the reviewing judge is so satisfied, the order issued shall specify:

(1) 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;

(2) The identity, if known, of the person who is the subject of the criminal investigation;

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

(4) A statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates; and

(5) Upon the request of the applicant, the information, facilities, and technical assistance necessary to accomplish installation of the pen register or trap and trace device that the provider of wire communication service is directed to furnish to the applicant.

(c) An order authorizing installation and use of a pen register or a trap and trace device shall not be for a period exceeding sixty days. Extension of such an order may be granted, but only upon a reapplication for an order and a finding of probable cause to justify continuing use of a pen register or trap and trace device. The period of the extension shall not exceed sixty days.

(d) An order authorizing 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 court; and

(2) The person owning or leasing the line to which the pen register or trap and trace device is attached, or who has been ordered by the court 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 other person, unless otherwise ordered by the court.

§803- Application for authorization to install and use a mobile tracking device. (a) A search warrant or court order must be obtained from the circuit court judge designated by the chief justice of the Hawaii supreme court or any other circuit court judge or district court judge, if a circuit court judge has not been designated by the chief justice of the Hawaii supreme court, or is otherwise unavailable, to install a mobile tracking device. Such order may authorize the use of that device within the jurisdiction of the court and outside that jurisdiction, if the device is installed in that jurisdiction.

(b) Upon application to the reviewing judge for a court order, the reviewing judge should satisfy itself that there are sufficient facts and circumstances contained within the application to establish probable cause to believe that the use of a mobile tracking device will discover the fruits, instrumentalities, or evidence of a crime or is relevant to an ongoing criminal investigation.

(c) If the designated judge is so satisfied, it shall issue an order specifying:

(1) The identity, if known, of the person who is the subject of the investigation;
(2) The number of mobile tracking devices to be used and the geographical location(s) where the devices are to be installed; and
(3) The identity, if known, of any person who may have a privacy interest in the point of installation of the mobile tracking device.

(d) An order authorizing installation and use of a mobile tracking device shall not exceed sixty days. Extensions of such orders may be granted only upon reapplication establishing probable cause to justify the continued use of a mobile tracking device. The period of the extension shall not exceed sixty days.

(e) The order shall direct that the order be sealed until otherwise directed by the court."

SECTION 3. Section 803-41, Hawaii Revised Statutes, is amended to read as follows:

"**§803-41 Definitions.** In this part:

"Aggrieved person" means a person who was party to any intercepted wire, [wireless, or] oral, or electronic communication or a person against whom the interception was directed.

"Aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

"Contents" when used with respect to any wire [or wireless], oral, or electronic communication, includes any information concerning the [identity of the parties to such communication or the existence,] substance, purport, or meaning of that communication.

"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 intrastate, interstate, or foreign commerce. The term "electronic communication" includes, but is not limited to, "display pagers" which can display visual message as part of the paging process, but does not include:

(1) The radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;
(2) Any wire or oral communication;
(3) Any communication made through a tone-only paging device; or
(4) Any communication from a tracking device.

"Electronic communication system" means any wire, radio, electromagnetic, photooptical, or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

"Electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, [wireless, or] oral, or electronic communication other than:

(1) Any telephone or telegraph instrument, equipment or facility, or any component thereof, (A) furnished to the subscriber or user by a [communications common carrier] 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 such subscriber or user for connection to the facilities of such services and used in the ordinary course of its business; or (B) being used by a [communications common carrier] 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; or

(2) A hearing aid or similar device being used to correct subnormal hearing to not better than normal.

"Electronic storage" means:

(1) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(2) Any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

"Intercept" means the aural or other acquisition of the contents of any wire [or wireless], electronic, or oral communication through the use of any electronic, mechanical, or other device.

"Investigative or law enforcement officer" means any officer of the State or political subdivision thereof, who is empowered by the law of this State to conduct investigations of or to make arrests for offenses enumerated in this part.

"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 such term does not include any electronic communication.

"Organized crime" means any combination or conspiracy to engage in criminal activity.

"Pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communication services provided by such provider or any device used by a provider or customer of a wire communication service, for cost accounting or other like purposes in the ordinary course of its business.

"Person" means any official, employee, or agent of the United States or this State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.

"Readily accessible to the general public" means, with respect to radio communication, that such communication is not:

(1) Scrambled or encrypted;

(2) Transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(3) Carried on a subcarrier or other signal subsidiary to a radio transmission;

(4) Transmitted over a communication system provided by a common carrier, unless the communication is a tone-only paging system communication; or

(5) Transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless in the case of a communication transmitted on a frequency allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.

"Tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object.

"Trap and trace device" means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

"User" means any person or entity who:

(1) Uses an electronic communication service; and
(2) Is duly authorized by the provider of such service to engage in such use.

"Wire communication" means any [communication] 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 [as a common carrier] in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications. The term "wire communication" includes, but is not limited to, cellular telephones, cordless telephones, except for the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, "tone and voice" pagers which transmit a voice message along with a paging signal, and any electronic storage of a wire communication.

["Wireless communication" means any communication made in whole or in part through the use of domestic public cellular radio telecommunications facilities or microwave facilities furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of intrastate, interstate, or foreign communications as defined and authorized by the Federal Communications Commission.]"

SECTION 4. Section 803-42, Hawaii Revised Statutes, is amended to read as follows:

"§803-42 Interception, access,[1] and disclosure of wire, [wireless,] oral, or electronic communications, use of pen register, trap and trace device, and mobile tracking device prohibited. (a) Except as otherwise specifically provided in this part any person who:

(1) [Wilfully] Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, [wireless, or] oral, or electronic communication;
(2) [Wilfully] 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, [wireless, or] oral, or electronic communication;
(3) [Wilfully] Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, [wireless, or] oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, [wireless, or] oral, or electronic communication in violation of this [subsection; or] part;
(4) [Wilfully] Intentionally uses, or endeavors to use, the contents of any wire, [wireless, or] oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, [wireless, or] oral, or electronic communication in violation of this [subsection;] 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 installs or uses a pen register or a trap and trace device without first obtaining a court order; or

(7) 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;

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 [any communication common carrier,] a provider of wire or electronic communication services, whose facilities are used in the transmission of a wire [or wireless] 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 which is 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 [carrier] provider of [such communication;] that service; provided that such [communication common carriers] 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 chapter 5 of title 47 of the United States Code, to intercept a wire or [wireless] electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(3) It shall not be unlawful under this part for a person not acting under color of law to intercept a wire, [wireless, or] oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such 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 [or for the purpose of committing any other injurious act]; provided that installation in any private place, without consent of the person or persons entitled to privacy therein, of any device for recording, amplifying, or broadcasting sounds or events in that place, or use of any such unauthorized installation, or installation or use outside a private place of such device to intercept sounds originating in that place which would not ordinarily be audible or comprehensible outside, without the consent of the person or persons entitled to privacy therein is prohibited.

(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 such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

[(4)] (5) It shall not be unlawful under this part for any person to intercept a wire, [wireless, or] 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 as otherwise authorized by law; provided that a communications [carrier] provider with knowledge of an interception of communications accomplished through the use of the communications [carrier's] 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, 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 an authorizing 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 such electronic communication is readily accessible to the general public.

(B) To intercept any radio communication which 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, civil defense, 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 which:

(i) Is prohibited by section 633 of the Communications Act of 1934; or

(ii) Is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act.

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

(E) For 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 such system, if such 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 such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from 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 such 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.

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

(10) 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;

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

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

(D) Which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if divulged to a law enforcement agency."

SECTION 5. Section 803-43, Hawaii Revised Statutes, is amended to read as follows:

"**§803-43 Devices to intercept wire, [wireless, or] oral, or electronic communications and advertising of same prohibited; penalty; [confiscation.] forfeiture.** Any person, other than a [communications or other common carrier] provider of wire or electronic communication service and its duly authorized officers [and], employees, and agents, or any person acting under color of law, who, in this State, intentionally manufactures, assembles, possesses, or distributes, or who attempts to distribute, any electronic, mechanical, or other device, knowing or having reason to know that the device or the design of the device renders it primarily useful for the purpose of [wiretapping, wire interception, wireless interception, or eavesdropping,] surreptitious interception of wire, oral, or electronic communica-

tions, or who intentionally places an advertisement of any such device or promotes the use of any such device in any newspaper, magazine, handbill, or other publication, shall be guilty of a class C felony. [Any police officer may confiscate any such electronic, mechanical, or other device in violation of this section, and upon conviction the devices shall be destroyed or otherwise disposed of as ordered by the court.] Any such electronic, mechanical, or other device in violation of this section shall be subject to seizure and forfeiture under title 37."

SECTION 6. Section 803-44, Hawaii Revised Statutes, is amended to read as follows:

"**§803-44 Application for court order to intercept wire [or wireless], oral, or electronic communications.** The attorney general of this State, or a designated deputy attorney general in the attorney general's absence or incapacity, or the prosecuting attorney of each county, or a designated deputy prosecuting attorney in the prosecuting attorney's absence or incapacity, may make application to a circuit court judge, designated by the chief justice of the Hawaii supreme court, or any other circuit court judge or district court judge, if a circuit court judge has not been designated by the chief justice of the Hawaii supreme court, or is otherwise unavailable, in the county where the interception is to take place, for an order authorizing or approving the interception of wire [or wireless], oral, or electronic communications, and such court may grant in conformity with section 803-46 an order authorizing, or approving the interception of wire [or wireless], oral, or electronic communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of murder, kidnapping, or felony criminal property damage involving the danger of serious bodily injury as defined in section 707-700, or involving organized crime and any of the following felony offenses: extortion; [criminal coercion;] bribery of a juror, of a witness, or of a police officer; receiving stolen property; gambling; and [sales] distribution of dangerous, harmful, or detrimental drugs."

SECTION 7. Section 803-45, Hawaii Revised Statutes, is amended to read as follows:

"**§803-45 Authorization for disclosure and use of intercepted wire [or wireless], oral, or electronic communications.** (a) Any investigative or law enforcement officer, who, by any means authorized by this part, has obtained knowledge of the contents of any wire, [wireless, or] 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 part, has obtained knowledge of the contents of any wire, [wireless, or] 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 officer's official duties.

(c) Any person who has received, by any means authorized by this part, any information concerning a wire, [wireless, or] oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this part 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 the grand jury in this State.

(d) No otherwise privileged wire, [wireless, or] oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this part shall lose its privileged character.

(e) When an investigative or law enforcement officer, while engaged in intercepting wire, [wireless, or] oral, or electronic communications in the manner authorized, intercepts communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (a) and (b) of this section. Such contents and any evidence derived therefrom may be used under subsection (c) of this section when authorized or approved by the designated circuit court where such court finds on subsequent application, made as soon as practicable, that the contents were otherwise intercepted in accordance with the provisions of this part.

(f) No testimony or evidence relating to a wire, [wireless or] oral, or electronic communication or any evidence derived therefrom intercepted in accordance with the provisions of this part shall be admissible in support of any misdemeanor charge."

SECTION 8. Section 803-46, Hawaii Revised Statutes, is amended to read as follows:

"**§803-46 Procedure for interception of wire [or wireless], oral, or electronic communication.** (a) Each application for an order authorizing or approving the interception of a wire [or wireless], oral, or electronic communication shall be made in writing upon oath or affirmation to a designated circuit court and shall state the applicant's authority to make such application. The terms "designated circuit," "designated judge," "authorized circuit court," "designated circuit court," "issuing judge," and the "court" as used in this section shall not only mean a circuit court judge specifically designated by the chief justice of Hawaii supreme court, but shall also mean any circuit court judge or district court judge if no circuit court judge has been designated by the chief justice, or is otherwise unavailable. Each application shall include the following information:

(1) The identity of the investigative or law enforcement officer(s) requesting the application, the official(s) applying for [a wiretap] an order;

(2) A full and complete statement of the facts and circumstances relied upon by the applicant, to justify the applicant's belief that an order should be issued, including (A) details as to the particular offense that has been, is being, or is about to be committed, (B) 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, (D) the identity or descriptions[1] of all persons, if known, committing[1] and whose communications are to be intercepted, and where appropriate (E) the involvement of organized crime;

(3) A full and complete statement of the facts concerning how the interception is to be accomplished, and if physical entry upon private premises is necessary, facts supporting such necessity;

(4) A full and complete statement of facts 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;

(5) A statement of facts indicating 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 ob-

tained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(6) A full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any court for authorization to intercept, or for approval of interceptions of, wire [or wireless], oral, or electronic communications involving any of the same persons, facilities, or places specified in the application, and the action taken by the court on each such application; and

(7) 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.

(b) An in camera adversary hearing shall be held on any [wiretap] interception application or application for extension. Upon receipt of the application the designated judge shall appoint an attorney to oppose the application. The attorney shall be appointed and compensated in the same manner as attorneys are appointed to represent indigent criminal defendants. The appointed attorney shall be given at least twenty-four hours notice of the hearing and shall be served with copies of the application, proposed order, if any, and supporting documents with the notice. At the hearing, the attorney appointed may cross-examine witnesses and present arguments in opposition to the application. The affiant supporting the application shall be present at the hearing. If an interlocutory appeal is taken by the State from the denial of an application, the appointed attorney shall be retained to answer the appeal or another attorney shall be appointed for the appeal. The designated circuit court may require the applicant to furnish additional testimony or documentary evidence under oath or affirmation in support of the application. A transcript of the hearing shall be made and kept with the application and orders.

(c) Upon such application and after such adversary hearing, the court may enter an order, as requested or as modified, authorizing or approving interception of wire [or wireless], oral, or electronic communications within the county in which the court is sitting, if the court 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 murder, kidnapping, or felony criminal property damage involving the danger of serious bodily injury or that an individual is committing, has committed, or is about to commit one of the other offenses specified in section 803-44 and that organized crime is involved;

(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) There is probable cause for belief that the facilities from which, or the place where, the wire [or wireless], 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 such person.

If the order allows physical entry to accomplish the interception, the issuing judge shall find that the interception could not be accomplished by means other than physical entry.

(d) Each order authorizing or approving the interception, of any wire [or wireless], oral, or electronic communication shall specify:

(1) The identity or description of all persons, 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 shall 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 the persons applying for the application;
(5) The period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained; and
(6) How the authorization is to be accomplished.

An order authorizing the interception of a wire [or wireless], oral, or electronic communication shall, upon request of the applicant, direct that a [communication common carrier] provider of wire or electronic communication service, landlord, custodian, or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such [carrier,] provider of wire or electronic communication service, landlord, custodian, or person is according the person whose communications are to be intercepted. Any [communication common carrier,] provider of wire or electronic communication service, landlord, custodian, or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant at the prevailing rates.

(e) No order entered under this section shall authorize or approve the interception of any wire [or wireless], oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. The thirty-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 ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsections (a) and (b) of this section and the court making the findings required by subsection (c) of this section. The period of extension shall be no longer than the authorizing circuit court deems necessary to achieve the purposes for which it was granted and in no event for longer than fifteen days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this part, and shall terminate upon attainment of the authorized objective, or in any event in thirty days or in fifteen days in case of an extension. In the event the intercepted communication is in a code or a 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 such interception. An interception may be conducted in whole or in part by investigative or law enforcement officer(s), or by an individual operating under contract, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.

(1) The interception shall be conducted in such a way as to minimize the resulting invasion of privacy including but not limited to the following methods of minimization:
    (A) Conversations that appear unlikely to result in incriminating conversations relating to the offense for which the order is issued shall be subject to intermittent monitoring; and

(B) Privileged conversations, including those between a person and the person's spouse, attorney, physician, or clergyman, shall not be intercepted unless both parties to the conversation are named or described in the [wiretap] application and order.

(2) In determining whether incriminating statements are likely to occur during a conversation the following factors should be considered:
(A) The parties to the conversation;
(B) The particular offense being investigated;
(C) The subject matter of the conversation;
(D) The subject matter of previous conversations between the same parties and whether any incriminating statements occurred; and
(E) The hour and day of conversation.

(f) Whenever an order authorizing interception is entered pursuant to this part, the order shall require reports to be made to the court which issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the court may require.

(g) (1) The contents of any wire [or wireless], oral, or electronic communication intercepted by any means authorized by this part shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire [or wireless], oral, or electronic communication under this subsection shall 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, such recordings shall be made available to the court issuing such order and sealed under the court's directions. Custody of the recordings shall be wherever the court orders. Recordings and other evidence of the contents of conversations and applications and orders shall not be destroyed except upon [the expiration of the statute of limitations for the particular offense for which the order was issued: six years in the case of class A felonies and three years in the case of class B and C felonies.] an order of the issuing or denying court and in any event shall be kept for ten years. However, upon the request of all the parties to particular conversations, evidence of conversations between those parties shall be destroyed (A) if there are no incriminating statements; (B) if any incriminating statements relate to only misdemeanor offenses; or (C) if the interception of the conversations is determined to have been illegal. Duplicate recordings may be made for use or disclosure pursuant to [the provisions of sections] section 803-45(a) and (b) for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire [or wireless], oral, or electronic communication or evidence derived therefrom under section 803-45(c).

(2) Applications made and orders granted under this part, transcripts of hearings on applications, and evidence obtained through court-ordered [wiretaps] interceptions shall be sealed by the designated circuit court. Custody of the above shall be whenever the court directs.

(3) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying court.

(4) Within a reasonable time but no later than ninety days after the termination of the period of an order or extensions thereof, the issuing court shall cause to be served, on the persons named in the order, on all other known parties to intercepted communications, and to such

other persons as the court may determine is in the interest of justice, an inventory which shall include notice of:

(A) The fact of the entry of the order;

(B) The date of the entry and the period of authorized, or approved interception;

(C) The fact whether during the period wire [or wireless], oral, or electronic communications were intercepted; and

(D) The fact whether any incriminating statements were intercepted.

The designated circuit court, upon the filing of a motion, shall make available to such person or the person's counsel for inspection after the inventory has been served all portions of the intercepted communications which contain conversations of that person, applications, orders, transcripts of hearing, and other evidence obtained as a result of the use of [wiretap] interception orders. The court may order such additional disclosure as the court determines to be in the interest of justice. On an ex parte showing of good cause to a court the serving of the inventory required by this subsection may be postponed.

(h) The contents of any intercepted wire [or wireless], oral, or electronic communication or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing,[1] or other proceeding in any court of this State unless each party, not less than thirty days before the trial, hearing or proceeding, has been furnished with copies of the documents required to be disclosed, and contents of intercepted communications or other evidence obtained as a result of [wiretapping] interception which is sought to be admitted in evidence. This thirty-day period may be shortened or waived by the court if it finds that the party will not be prejudiced by the delay in receiving such information.

(i) (1) 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 content of any intercepted wire [or wireless], oral, or electronic communication, or evidence derived therefrom, on the grounds that:

(A) The communication was unlawfully intercepted;

(B) The order of authorization or approval under which it was intercepted is insufficient on its face; or

(C) The interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceedings unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or wireless communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this part. The court, or other official before whom the motion is made, upon the filing of such motion by the aggrieved person, shall make available to the aggrieved person or the aggrieved person's counsel for inspection portions of the recording which contain intercepted communications of the defendant or evidence derived therefrom, the applications, orders, transcript of hearing, and such additional evidence as the court determines to be in the interest of justice.

(2) In addition to any other right to appeal the State shall have the right to appeal:

(A) From an order granting a motion to suppress made under paragraph (1) of this subsection if the attorney general or prosecuting attorney, or their designated representatives, shall certify to the

court or other official granting such motion that the appeal shall be taken within thirty days after the date the order of suppression was entered and shall be diligently prosecuted as in the case of other interlocutory appeals or under such rules as the supreme court may adopt;

(B) From an order denying an application for an order of authorization or approval, and such an appeal shall be in camera and in preference to all other pending appeals in accordance with rules promulgated by the supreme court."

SECTION 9. Section 803-47, Hawaii Revised Statutes, is amended to read as follows:

"**§803-47 Reports concerning intercepted wire [or wireless], oral, or electronic communications.** (a) In January of each year, the attorney general and county prosecuting attorneys of this State shall report to the administrative director of the courts of this State and to the administrative office of the United States Courts:

(1) The fact that an order or extension was applied for;
(2) The kind of order or extension applied for;
(3) The fact that the order or extension was granted as applied for, was modified, or was denied;
(4) The period of interceptions authorized by the order, and the number and duration of any extensions of the order;
(5) The offense specified in the order or application, or extension of an order;
(6) The identity of the investigative or law enforcement officer and agency requesting the application and the person authorizing the request for application;
(7) The nature of the facilities from which or the place where communications were to be intercepted;
(8) A general description of the interceptions made under such order or extension, including (A) the approximate nature and frequency of incriminating communications intercepted, (B) the approximate nature and frequency of other communications intercepted, (C) the approximate number of persons whose communications were intercepted, and (D) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;
(9) The number of arrests resulting from interceptions made under such order on extension, and the offenses for which arrests were made;
(10) The number of trials resulting from such interceptions;
(11) The number of motions to suppress made with respect to such interceptions, and the number granted or denied;
(12) The number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions;
(13) The information required by paragraphs (2) through (6) of this subsection with respect to orders or extensions obtained in a preceding calendar year and not yet reported; and
(14) Other information required by the rules and regulations of the administrative office of the United States Courts.

(b) In March of each year the administrative director of the courts shall transmit to the legislature a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire [or wire-

less], oral, or electronic communications and the number of orders and extensions granted or denied during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the administrative director of the courts by the attorney general and prosecuting attorneys."

SECTION 10. Section 803-48, Hawaii Revised Statutes, is amended to read as follows:

"**§803-48 Recovery of civil damages authorized.** Any person whose wire, [wireless, or] oral, or electronic communication is accessed, intercepted, disclosed, or used in violation of this part shall (1) have a civil cause of action against any person who accesses, intercepts, discloses, or uses, or procures any other person to access, intercept, disclose, or use such communications, and (2) be entitled to recover from any such person:

(A) [Actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation;] The greater of (i) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, or (ii) statutory damages of whichever is the greater of $100[1] day for each day of violation or $10,000;

(B) Punitive damages[;], where appropriate; and

(C) A reasonable attorney's fee and other litigation costs reasonably incurred.

The aggrieved person may also seek and be awarded such preliminary, and other equitable or declaratory relief as may be appropriate. A good faith reliance on a court order shall constitute a complete defense to any civil action brought under this part."

SECTION 11. Statutory material to be repealed is bracketed. New statutory material is underscored.[2]

SECTION 12. This Act shall take effect upon its approval.

(Approved June 7, 1989.)

Notes

1. So in original.
2. Edited pursuant to HRS §23G-16.5.