

**Report Title:**

Electronic Surveillance; Wiretapping

**Description:**

Amends State's electronic eavesdropping statute. (SB965 HD1)



---

---

# A BILL FOR AN ACT

RELATING TO ELECTRONIC SURVEILLANCE.

**BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:**

1 SECTION 1. Chapter 28, Hawaii Revised Statutes, is amended by  
2 adding a new section to be appropriately designated and to read  
3 as follows:  
4 "§28- Surveillance review unit. There is established in  
5 the department of the attorney general a surveillance review  
6 unit, which shall be responsible for reviewing all applications  
7 for interception of wire, oral, or electronic communications  
8 under chapter 803 prior to their submittal to a designated  
9 judge, regardless of whether submitted by county or state  
10 investigative or law enforcement officers. A surveillance  
11 review unit deputy attorney general shall review the application  
12 in a timely manner to ensure it meets the requirements of part  
13 IV of chapter 803 and applicable law and recommend any necessary  
14 additions or changes to the application. Thereafter, the  
15 surveillance review unit deputy attorney general shall prepare a  
16 written memorandum recommending approval or disapproval of the  
17 application, which shall be submitted to the district court  
18 judge or designated judge with the application. The attorney



1 general shall establish standards and procedures for the timely  
2 review of these applications to ensure continuity and conformity  
3 with applicable law."

4 SECTION 2. Chapter 803, part IV, Hawaii Revised Statutes,  
5 is amended to read as follows:

6 "PART IV. ELECTRONIC EAVESDROPPING

7 §803-41 Definitions. As used in [H] this part, unless  
8 the context clearly requires otherwise:

9 "Aggrieved person" means a person who was party to any  
10 intercepted wire, oral, or electronic communication or a person  
11 against whom the interception was directed.

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

15 "Bait vehicle" means any vehicle used by law enforcement to  
16 further an investigation of and deter unauthorized entry into a  
17 motor vehicle or unauthorized control of propelled vehicles.

18 [~~"Aural transfer" means a transfer containing the human~~  
19 ~~voice at any point between and including the point of origin and~~  
20 ~~the point of reception.]~~

21 "Communication common carrier" means any person engaged as  
22 a common carrier for hire in interstate or foreign communication



1 by wire or radio or in intrastate, interstate, or foreign radio  
2 transmission of energy, except where reference is made to  
3 communication common carriers not subject to this part; provided  
4 that a person engaged in radio broadcasting, to the extent the  
5 person is so engaged, shall not be deemed a communication common  
6 carrier.

7 "Contents" when used with respect to any wire, oral, or  
8 electronic communication, includes any information concerning  
9 the substance, purport, or meaning of that communication.

10 "Designated judge" means a circuit court judge designated  
11 by the chief justice of the Hawaii supreme court to issue orders  
12 under this part.

13 "Electronic communication" means any transfer of signs,  
14 signals, writing, images, sounds, data, or intelligence of any  
15 nature transmitted in whole or in part by a wire, radio,  
16 electromagnetic, photoelectronic, or [~~photooptical~~] photo-  
17 optical system that affects intrastate, interstate, or foreign  
18 commerce. The term "electronic communication" includes, but is  
19 not limited to, "display pagers" which can display visual  
20 message as part of the paging process, but does not include:



1       (1) ~~[The radio portion of a cordless telephone~~  
2           ~~communication that is transmitted between the cordless~~  
3           ~~telephone handset and the base unit;~~

4       ~~(2)]~~ Any wire or oral communication;

5       (~~3]~~2) Any communication made through a tone-only paging  
6           device; ~~[or]~~

7       (~~4]~~3) Any communication from a tracking device~~[-]~~; or

8       (4) Electronic funds transfer information stored by  
9           financial institution in a communications system used  
10          for the electronic storage and transfer of funds.

11       "Electronic communication service" means any service that  
12 provides to users thereof the ability to send or receive wire or  
13 electronic communications.

14       "Electronic communication system" means any wire, radio,  
15 electromagnetic, ~~[photooptical]~~ photo-optical, or  
16 photoelectronic facilities for the transmission of electronic  
17 communications, and any computer facilities or related  
18 electronic equipment for the electronic storage of ~~[such]~~ these  
19 communications.

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



1 (1) Any telephone or telegraph instrument, equipment or  
2 facility, or any component thereof, (A) furnished to  
3 the subscriber or user by a provider of wire or  
4 electronic commu0nication service in the ordinary  
5 course of its business and being used by the  
6 subscriber or user in the ordinary course of its  
7 business or furnished by [~~such~~] the subscriber or user  
8 for connection to the facilities of [~~such~~] the  
9 services and used in the ordinary course of its  
10 business; or (B) being used by a provider of wire or  
11 electronic communication service in the ordinary  
12 course of its business, or by an investigative or law  
13 enforcement officer in the ordinary course of the  
14 officer's duties; or

15 (2) A hearing aid or similar device being used to correct  
16 subnormal hearing to a level not better than [~~normal~~]  
17 average.

18 "Electronic storage" means:

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



1           (2) Any storage of [~~such~~] the communication by an  
2                    electronic communication service for purposes of  
3                    backup protection of [~~such~~] the communication.

4            "Intercept" means the aural or other acquisition of the  
5            contents of any wire, electronic, or oral communication through  
6            the use of any electronic, mechanical, or other device.

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

11           "Oral communication" means any [~~oral communication uttered~~]  
12           utterance by a person exhibiting an expectation that [~~such~~  
13           ~~communication~~] the utterance is not subject to interception  
14           under circumstances justifying [~~such~~] that expectation, but  
15           [~~such~~] the term does not include any electronic communication.

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

18           "Pen register" means a device [~~which~~] that records or  
19           decodes electronic or other impulses [~~which~~] that identify the  
20           numbers dialed or otherwise transmitted on the telephone line to  
21           which such device is attached, but [~~such~~] the such term does not  
22           include any device used by a provider or customer of a wire or



1 electronic communication service for billing, or recording as an  
2 incident to billing, for communication services provided by  
3 [~~such~~] the provider or any device used by a provider or customer  
4 of a wire communication service[7] for cost accounting or other  
5 [~~like~~] similar purposes in the ordinary course of its business.

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

10 "Readily accessible to the general public" means, with  
11 respect to radio communication, that [~~such~~] the communication is  
12 not:

- 13 (1) Scrambled or encrypted;
- 14 (2) Transmitted using modulation techniques whose  
15 essential parameters have been withheld from the  
16 public with the intention of preserving the privacy of  
17 [~~such~~] the communication;
- 18 (3) Carried on a subcarrier or other signal subsidiary to  
19 a radio transmission;
- 20 (4) Transmitted over a communication system provided by a  
21 common carrier, unless the communication is a tone-  
22 only paging system communication; or





1 (5) Transmitted on frequencies allocated under part 25,  
2 subpart D, E, or F of part 74, or part 94 of the Rules  
3 of the Federal Communications Commission, unless in  
4 the case of a communication transmitted on a frequency  
5 allocated under part 74 that is not exclusively  
6 allocated to broadcast auxiliary services, the  
7 communication is a two-way voice communication by  
8 radio.

9 "Remote computing service" means the provision to the  
10 public of computer storage or processing services by means of an  
11 electronic communication system.

12 "Tracking device" means an electronic or mechanical device  
13 [~~which~~] that permits the tracking of the movement of a person or  
14 object, but does not include [~~such~~] a device when installed:

15 (1) In a motor vehicle or other vehicle by or with the  
16 permission of the owner or person in lawful possession  
17 of the motor vehicle or other vehicle for the purpose  
18 of tracking the movement of [~~such~~] the motor vehicle  
19 or other vehicle; or

20 (2) By or at the request of a police department or law  
21 enforcement agency in a "bait vehicle".



1 "Trap and trace device" means a device [~~which~~] that  
2 captures the incoming electronic or other impulses [~~which~~] that  
3 identify the originating number of an instrument or device from  
4 which a wire or electronic communication was transmitted.

5 "User" means any person or entity [~~who~~] that:

- 6 (1) Uses an electronic communication service; and  
7 (2) Is duly authorized by the provider of [~~such~~] the  
8 service to engage in such use.

9 "Wire communication" means any aural transfer made in whole  
10 or in part through the use of facilities for the transmission of  
11 communications by the aid of wire, cable, or other like  
12 connection between the point of origin and the point of  
13 reception (including the use of such connection in a switching  
14 station) furnished or operated by any person engaged in  
15 providing or operating such facilities for the transmission of  
16 intrastate, interstate, or foreign communications. The term  
17 "wire communication" includes, but is not limited to, cellular  
18 telephones, cordless telephones, except for the radio portion of  
19 a cordless telephone communication that is transmitted between  
20 the cordless telephone handset and the base unit, "tone and  
21 voice" pagers which transmit a voice message along with a paging  
22 signal, and any electronic storage of a wire communication.



1           §803-42   Interception, access, and disclosure of wire,  
2 oral, or electronic communications, use of pen register, trap  
3 and trace device, and mobile tracking device prohibited. (a)

4 Except as otherwise specifically provided in this part, any  
5 person who:

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

10          (2) Intentionally uses, endeavors to use, or procures any  
11          other person to use or endeavor to use any electronic,  
12          mechanical, or other device to intercept any wire,  
13          oral, or electronic communication;

14          (3) Intentionally discloses, or endeavors to disclose, to  
15          any other person the contents of any wire, oral, or  
16          electronic communication, knowing or having reason to  
17          know that the information was obtained through the  
18          interception of a wire, oral, or electronic  
19          communication in violation of this part;

20          (4) Intentionally uses, or endeavors to use, the contents  
21          of any wire, oral, or electronic communication,  
22          knowing or having reason to know that the information



1 was obtained through the interception of a wire, oral,  
2 or electronic communication in violation of this part;

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

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

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

16 (A) Either:

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



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

3                                   and

4                   (B) With the intent to improperly obstruct, impede,  
5                                   or interfere with a duly authorized criminal  
6                                   investigation.

7                   ([6]7) Intentionally installs or uses a pen register or a  
8                                   trap and trace device without first obtaining a court  
9                                   order; or

10                   ([7]8) Intentionally installs or uses a mobile tracking  
11                                   device without first obtaining a search warrant or  
12                                   other order authorizing the installation and use of  
13                                   such device;

14 shall be guilty of a class C felony.

15                   (b)   (1) It shall not be unlawful under this part for an  
16                                   operator of a switchboard, or an officer, employee, or  
17                                   agent of a provider of wire or electronic  
18                                   communication services, whose facilities are used in  
19                                   the transmission of a wire communication, to  
20                                   intercept, disclose, or use that communication in the  
21                                   normal course of the officer's, employee's, or agent's  
22                                   employment while engaged in any activity [~~which~~] that



1 is either a necessary incident to the rendition of the  
2 officer's, employee's, or agent's service or to the  
3 protection of the rights or property of the provider  
4 of that service; provided that [~~such~~] providers of  
5 wire communication service to the public shall not  
6 utilize service observing or random monitoring except  
7 for mechanical or service quality control checks.

8 (2) It shall not be unlawful under this part for an  
9 officer, employee, or agent of the Federal  
10 Communications Commission, in the normal course of the  
11 officer's, employee's, or agent's employment and in  
12 discharge of the monitoring responsibilities exercised  
13 by the Commission in the enforcement of [~~chapter 5 of~~]  
14 title 47, chapter 5, of the United States Code, to  
15 intercept a wire or electronic communication, or oral  
16 communication transmitted by radio, or to disclose or  
17 use the information thereby obtained.

18 (3) It shall not be unlawful under this part for a person  
19 not acting under color of law to intercept a wire,  
20 oral, or electronic communication [~~where such~~] when  
21 the person is a party to the communication or [~~where~~]  
22 when one of the parties to the communication has given



1 prior consent to [~~such~~] the interception unless [~~such~~]  
2 the communication is intercepted for the purpose of  
3 committing any criminal or tortious act in violation  
4 of the Constitution or laws of the United States or of  
5 this State; provided that installation by a person not  
6 acting under color of law in any private place,  
7 without consent of the person or persons entitled to  
8 privacy therein, of any device for recording,  
9 amplifying, or broadcasting sounds or events in that  
10 place, or use of any such unauthorized installation,  
11 or installation or use outside a private place of such  
12 device to intercept sounds originating in that place  
13 which would not ordinarily be audible or  
14 comprehensible outside, without the consent of the  
15 person or persons entitled to privacy therein is  
16 prohibited.

- 17 (4) It shall not be unlawful under this part for a person  
18 acting under color of law to intercept a wire, oral,  
19 or electronic communication, when [~~such~~] the person is  
20 a party to the communication or one of the parties to  
21 the communication has given prior consent to [~~such~~]  
22 the interception.



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

13          (6) Notwithstanding any other law to the contrary,  
14          providers of wire or electronic communication service,  
15          their officers, employees, and agents, landlords,  
16          custodians, or other persons, are authorized to  
17          provide information, facilities, or technical  
18          assistance to persons authorized by law to intercept  
19          or access wire, oral, or electronic communications, to  
20          conduct electronic surveillance, or to install a pen  
21          register or trap and trace device if such provider,  
22          its officers, employees, or agents, landlord,





1           custodian, or other specified person, has been  
2           provided with:

3           (A) A court order directing such assistance signed by  
4           ~~[an authorizing]~~ the designated judge; or

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

19                   No provider of wire or electronic  
20                   communication service, officer, employee, or  
21                   agent thereof, or landlord, custodian, or other  
22                   specified person shall disclose the existence of



1 any access, interception, or surveillance or the  
2 device used to accomplish the interception or  
3 surveillance for which the person has been  
4 furnished a court order or certification under  
5 this part, except as may otherwise be required by  
6 legal process and then only after prior  
7 notification to the party that provided the court  
8 order or certification.

9 No cause of action shall lie in any court  
10 against any provider of wire or electronic  
11 communication service, its officers, employees,  
12 or agents, landlord, custodian, or other  
13 specified person for providing information,  
14 facilities, or assistance in accordance with the  
15 terms of a court order or certification under  
16 this part.

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

19 (A) To intercept or access an electronic  
20 communication made through an electronic  
21 communication system configured so that [~~such~~]



1           the electronic communication is readily  
2           accessible to the general public.

3           (B) To intercept any radio communication [~~which~~] that  
4           is transmitted:

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

8           (ii) By any governmental, law enforcement, civil  
9           defense, private land mobile, or public  
10          safety communications system, including  
11          police and fire, readily accessible to the  
12          general public;

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

17          (iv) By any marine or aeronautical communications  
18          system.

19          (C) To engage in any conduct [~~which~~] that:

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

22          or



1 (ii) Is excepted from the application of section  
2 705(a) of the Communications Act of 1934 by  
3 section 705(b) of that Act (47 U.S.C. §605).

4 (D) To intercept any wire or electronic communication  
5 the transmission of which is causing harmful  
6 interference to any lawfully operating station or  
7 consumer electronic equipment to the extent  
8 necessary to identify the source of [~~such~~] the  
9 interference;

10 (E) For other users of the same frequency to  
11 intercept any radio communication made through a  
12 system that uses frequencies monitored by  
13 individuals engaged in the providing or the use  
14 of [~~such~~] the system, if [~~such~~] the communication  
15 is not scrambled or encrypted.

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

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

19 (B) For a provider of electronic communication  
20 service to record the fact that a wire or  
21 electronic communication was initiated or  
22 completed in order to protect [~~such~~] the



1 provider, another provider furnishing service  
2 toward the completion of the wire or electronic  
3 communication, or a user of that service, from  
4 the fraudulent, unlawful, or abusive use of such  
5 service.

6 (C) For a provider of electronic or wire  
7 communication service to use a pen register or a  
8 trap and trace device for purposes relating to  
9 the operation, maintenance, and testing of the  
10 wire or electronic communication service or to  
11 the protection of the rights or property of  
12 [~~such~~] the provider, or to the protection of  
13 users of that service from abuse of service or  
14 unlawful use of service.

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

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

21 (10) Except as provided in this section, a person or entity  
22 providing an electronic communication service to the



1           public shall not intentionally divulge the contents of  
2           any communication (other than a communication to the  
3           person or entity or an agent thereof) while in  
4           transmission on that service to any person or entity  
5           other than an addressee or intended recipient of the  
6           communication or an agent of the addressee or intended  
7           recipient.

8           A person or entity providing electronic communication  
9           service to the public may divulge the contents of any  
10          such communication:

- 11          (A) As otherwise authorized by a court order;
- 12          (B) With the lawful consent of the originator,  
13                addressee, [~~originator~~] or intended recipient of  
14                the communication;
- 15          (C) To a person employed or authorized, or whose  
16                facilities are used, to forward [~~such~~] the  
17                communication to its destination; or
- 18          (D) [~~which were~~] That was inadvertently obtained by  
19                the service provider and [~~which appear~~] that  
20                appears to pertain to the commission of a crime,  
21                if divulged to a law enforcement agency.



1        (11) It shall not be unlawful under this part for any  
2                    person to disclose an illegally intercepted  
3                    communication in the course of publication of truthful  
4                    information of public concern.

5            **§803-43 Devices to intercept wire, oral, or electronic**  
6 **communications and advertising of same prohibited; penalty;**  
7 **forfeiture.** Any person, other than a provider of wire or  
8 electronic communication service and its duly authorized  
9 officers, employees, and agents, or any person acting under  
10 color of law, who, in this State, intentionally manufactures,  
11 assembles, possesses, or distributes, or who attempts to  
12 distribute, any electronic, mechanical, or other device, knowing  
13 or having reason to know that the device or the design of the  
14 device renders it primarily useful for the purpose of  
15 surreptitious interception of wire, oral, or electronic  
16 communications, or who intentionally places an advertisement of  
17 any such device or promotes the use of any such device in any  
18 newspaper, magazine, handbill, or other publication, shall be  
19 guilty of a class C felony. Any such electronic, mechanical, or  
20 other device in violation of this section shall be subject to  
21 seizure and forfeiture under [~~title 37~~] chapter 712A.



1           **§803-44 Application for court order to intercept wire,**  
2 **oral, or electronic communications.** The attorney general of  
3 this State, or a designated deputy attorney general in the  
4 attorney general's absence or incapacity, or the prosecuting  
5 attorney of each county, or a designated deputy prosecuting  
6 attorney in the prosecuting attorney's absence or incapacity,  
7 may make application to a [~~circuit court judge,~~] designated  
8 judge [~~by the chief justice of the Hawaii supreme court,~~] or any  
9 other circuit court judge or district court judge, if a circuit  
10 court judge has not been designated by the chief justice of the  
11 Hawaii supreme court, or is otherwise unavailable, in the county  
12 where the interception is to take place, for an order  
13 authorizing or approving the interception of wire, oral, or  
14 electronic communications, and such court may grant in  
15 conformity with section 803-46 an order authorizing, or  
16 approving the interception of wire, oral, or electronic  
17 communications by investigative or law enforcement officers  
18 having responsibility for the investigation of the offense as to  
19 which the application is made, [~~when such~~] if the interception  
20 [~~may~~] might provide or has provided evidence of murder,  
21 kidnapping, or felony criminal property damage involving the  
22 danger of serious bodily injury as defined in section 707-700,





1 or involving organized crime and any of the following felony  
2 offenses: extortion; bribery of a juror, of a witness, or of a  
3 police officer; receiving stolen property; gambling; and  
4 distribution of dangerous, harmful, or detrimental drugs.

5 **[§8030-44.5] Application for a pen register or a trap and**  
6 **trace device.** (a) The attorney general of this State or the  
7 prosecuting attorney for each county, or a subordinate  
8 designated to act in either's absence or incapacity, may apply  
9 in writing under oath or equivalent affirmation to a [~~circuit~~  
10 ~~court judge~~] designated judge [~~by the chief justice of the~~  
11 ~~Hawaii supreme court~~] or any other circuit court judge or  
12 district court judge, if a circuit court judge has not been  
13 designated by the chief justice of the Hawaii supreme court, or  
14 is otherwise unavailable, for an order or an extension of an  
15 order to authorize the installation and use of a pen register or  
16 a trap and trace device.

17 (b) The application shall include:

18 (1) The identity of the official making the application  
19 and the law enforcement agency conducting the  
20 investigation; and

21 (2) The facts and circumstances relied upon by the  
22 applicant to conclude that there is probable cause to



1 believe that information will be obtained through the  
2 installation and use of a pen register or trap and  
3 trace device [~~which~~] that will constitute the fruits,  
4 instrumentalities, or evidence of a crime covered  
5 under this part.

6 **[§803-44.6] Issuance of an order for a pen register or a**  
7 **trap and trace device.** (a) Upon an application for an order  
8 authorizing the installation and use of a pen register or a trap  
9 and trace device, the [~~reviewing~~] designated judge shall satisfy  
10 itself that there are sufficient facts and circumstances  
11 contained within the application that there is is probable cause  
12 to believe that the information [~~will~~] to be obtained through  
13 the installation and use of a pen register or a trap and trace  
14 device [~~which~~] will constitute the fruits, instrumentalities, or  
15 evidence of a crime or is relevant to an ongoing criminal  
16 investigation.

17 (b) If the [~~reviewing~~] designated judge is so satisfied,  
18 the order issued:

19 (1) [~~shall~~] Shall specify:

20 (~~±~~)A) The identity, if known, of the person to  
21 whom is leased or in whose name is listed the



1 telephone line to which the pen register or trap  
2 and trace device is to be attached;

3 (~~2~~B) The identity, if known, of the person who is  
4 the subject of the criminal investigation;

5 (~~3~~C) The number and, if known, the physical  
6 location of the telephone line to which the pen  
7 register or the trap and trace device is to be  
8 attached, and, in the case of a trap and trace  
9 device, the geographical limits of the trap and  
10 trace order;

11 (~~4~~D) A statement of the offense to which the  
12 information likely to be obtained by the pen  
13 register or trap and trace device relates; and

14 (~~5~~2) Shall specify, [Upon] upon the request of the  
15 applicant, the information, facilities, and technical  
16 assistance necessary to accomplish the installation of  
17 the pen register or trap and trace device that the  
18 provider of wire communication service is directed to  
19 furnish to the applicant.

20 (c) An order authorizing installation and use of a pen  
21 register or a trap and trace device shall [~~not~~] be for a period  
22 [~~exceeding~~] not to exceed sixty days. Extension of [~~such~~] an



1 order may be granted, but only upon a reapplication for an order  
2 and a finding of probable cause to justify continuing use of a  
3 pen register or trap and trace device. The period of the  
4 extension shall be for a period not to exceed sixty days.

5 (d) An order authorizing the installation and use of a pen  
6 register or a trap and trace device shall direct that:

7 (1) The order be sealed until otherwise ordered by the  
8 court; and

9 (2) The person owning or leasing the line to which the pen  
10 register or trap and trace device is attached, or who  
11 has been ordered by the court to provide assistance to  
12 the applicant, not disclose the existence of the pen  
13 register or trap and trace device or the existence of  
14 the investigation to the listed subscriber[7] or to  
15 any other person, unless otherwise ordered by the  
16 court.

17 **[§803-44.7] Application for authorization to install and**  
18 **use a mobile tracking device.** (a) A search warrant or court  
19 order must be obtained from the [~~circuit court judge~~] designated  
20 judge [~~by the chief justice of the Hawaii supreme court~~] or any  
21 other circuit court judge or district court judge, if a circuit  
22 court judge has not been designated by the chief justice of the



1 Hawaii supreme court, or is otherwise unavailable, to install a  
2 mobile tracking device. [~~Such~~] The order may authorize the use  
3 of that device within the jurisdiction of the court and outside  
4 that jurisdiction, if the device is installed in that  
5 jurisdiction.

6 (b) If, [~~Upon~~] upon application to the [~~reviewing~~]  
7 designated judge for a court order, the [~~reviewing~~] designated  
8 judge should satisfy itself that there are sufficient facts and  
9 circumstances contained within the application to establish  
10 probable cause to believe that the use of a mobile tracking  
11 device will discover the fruits, instrumentalities, or evidence  
12 of a crime or is relevant to an ongoing criminal investigation.

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

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



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

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

9 **§803-45 Authorization for disclosure and use of**  
10 **intercepted wire, oral, or electronic communications.** (a) Any  
11 investigative or law enforcement officer, who, by any means  
12 authorized by this part, has obtained knowledge of the contents  
13 of any wire, oral, or electronic communication, or evidence  
14 derived therefrom, may disclose [~~such~~] the contents to another  
15 investigative or law enforcement officer to the extent that  
16 [~~such~~] the disclosure is appropriate to the proper performance  
17 of the official duties of the officer making or receiving the  
18 disclosure.

19 (b) Any investigative or law enforcement officer, who by  
20 any means authorized by this part, has obtained knowledge of the  
21 contents of any wire, oral, or electronic communication or  
22 evidence derived therefrom may use [~~such~~] the contents to the



1 extent [~~such~~] the use is appropriate to the proper performance  
2 of the officer's official duties.

3 (c) Any person who has received, by any means authorized  
4 by this part, any information [~~concerning~~] from a wire, oral, or  
5 electronic communication, or evidence derived therefrom  
6 intercepted in accordance with the provisions of this part may  
7 disclose the contents of that communication or [~~such~~] any  
8 derivative evidence while giving testimony under oath or  
9 affirmation in any proceeding in any court or before the grand  
10 jury in this State.

11 (d) No otherwise privileged wire, oral, or electronic  
12 communication intercepted in accordance with, or in violation  
13 of, the provisions of this part shall lose its privileged  
14 character.

15 (e) When an investigative or law enforcement officer,  
16 while engaged in [~~intercepting~~] authorized interception,  
17 intercepts wire, oral, or electronic communications [~~in the~~  
18 ~~manner authorized, intercepts communications~~] relating to  
19 offenses other than those specified in the order of  
20 authorization or approval, the contents thereof, and evidence  
21 derived therefrom, may be disclosed or used as provided in  
22 subsections (a) and (b) of this section. [~~Such~~] The contents



1 and any evidence derived therefrom may be used under subsection  
2 (c) of this section when authorized or approved by the  
3 designated [~~circuit court~~] judge where [~~such court~~] the judge  
4 finds on subsequent application, made as soon as practicable,  
5 that the contents were otherwise intercepted in accordance with  
6 the provisions of this part.

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

11 **§803-46 Procedure for interception of wire, oral, or**  
12 **electronic communication.** (a) Each application for an order  
13 authorizing or approving the interception of a wire, oral, or  
14 electronic communication shall be made in writing upon oath or  
15 affirmation to a designated [~~circuit court~~] judge and shall be  
16 accompanied by a written memorandum recommending approval or  
17 disapproval by the department of attorney general. The  
18 application shall state the applicant's authority to make [~~such~~]  
19 the application. The [~~terms~~] term [~~"designated circuit,"~~]  
20 "designated judge[~~]~~" [~~"authorized circuit court," "designated~~  
21 ~~circuit court," "issuing judge," and the "court"~~] as used in  
22 this section shall not only mean a circuit court judge





1 specifically designated by the chief justice of Hawaii supreme  
2 court, but shall also mean any circuit court judge or district  
3 court judge if no circuit court judge has been designated by the  
4 chief justice, or is otherwise unavailable. Each application  
5 shall include the following information:

6 (1) The identity of the investigative or law enforcement  
7 officer(s) requesting the application, the official(s)  
8 applying for an order;

9 (2) A full and complete statement of the facts and  
10 circumstances relied upon by the applicant, to justify  
11 the applicant's belief that an order should be issued,  
12 including (A) details as to the particular offense  
13 that has been, is being, or is about to be committed,  
14 (B) a particular description of the nature and  
15 location of the facilities from which or the place  
16 where the communication is to be intercepted, (C) a  
17 particular description of the type of communications  
18 sought to be intercepted, (D) the identity or  
19 descriptions of all persons, if known, committing the  
20 offense and whose communications are to be  
21 intercepted, and where appropriate (E) the involvement  
22 of organized crime;



- 1           (3) A full and complete statement of the facts concerning  
2           how the interception is to be accomplished, and if  
3           physical entry upon private premises is necessary,  
4           facts supporting such necessity;
- 5           (4) A full and complete statement of facts as to whether  
6           or not other investigative procedures have been tried  
7           and failed or why they reasonably appear to be  
8           unlikely to succeed if tried or to be too dangerous;
- 9           (5) A statement of facts indicating the period of time for  
10          which the interception is required to be maintained.  
11          If the nature of the investigation is such that the  
12          authorization for interception should not  
13          automatically terminate when the described type of  
14          communication has been obtained, a particular  
15          description of facts establishing probable cause to  
16          believe that additional communications of the same  
17          type will occur thereafter;
- 18          (6) A full and complete statement of the facts concerning  
19          all previous applications known to the individual  
20          authorizing and making the application, made to any  
21          [~~court~~] designated judge for authorization to  
22          intercept, or for approval of interceptions of, wire,



1 oral, or electronic communications involving any of  
2 the same persons, facilities, or places specified in  
3 the application, and the action taken by the [court]  
4 designated judge on each [~~such~~] application; and

5 (7) [~~Where~~] When the application is for the extension of  
6 an order, a statement setting forth the results thus  
7 far obtained from the interception, or a reasonable  
8 explanation of the failure to obtain [~~such~~] any  
9 results.

10 (b) [~~An in camera adversary hearing shall be held on any~~  
11 ~~interception application or application for extension. Upon~~  
12 ~~receipt of the application the designated judge shall appoint an~~  
13 ~~attorney to oppose the application. The attorney shall be~~  
14 ~~appointed and compensated in the same manner as attorneys are~~  
15 ~~appointed to represent indigent criminal defendants. The~~  
16 ~~appointed attorney shall be given at least twenty-four hours~~  
17 ~~notice of the hearing and shall be served with copies of the~~  
18 ~~application, proposed order, if any, and supporting documents~~  
19 ~~with the notice. At the hearing, the attorney appointed may~~  
20 ~~cross-examine witnesses and present arguments in opposition to~~  
21 ~~the application. The affiant supporting the application shall~~  
22 ~~be present at the hearing. If an interlocutory appeal is taken~~



1 ~~by the State from the denial of an application, the appointed~~  
2 ~~attorney shall be retained to answer the appeal or another~~  
3 ~~attorney shall be appointed for the appeal.]~~ The designated  
4 [~~circuit court~~] judge may require the applicant to furnish  
5 [~~additional~~] testimony or documentary evidence under oath or  
6 affirmation in support of the application. A transcript of the  
7 hearing shall be made and kept with the application and orders.

8 (c) Upon [~~such~~] an application [~~and after such adversary~~  
9 ~~hearing,~~] the [~~court~~] designated judge may enter an ex parte  
10 order, as requested or as modified, authorizing or approving  
11 interception of wire, oral, or electronic communications within  
12 the county in which the [~~court~~] designated judge is sitting, if  
13 the [~~court~~] designated judge determines on the basis of the  
14 facts submitted by the applicant that:

15 (1) There is probable cause [~~for belief~~] to believe that  
16 an individual is committing, has committed, or is  
17 about to commit murder, kidnapping, or felony criminal  
18 property damage involving the danger of serious bodily  
19 injury or that an individual is committing, has  
20 committed, or is about to commit one of the other  
21 offenses specified in section 803-44 and that  
22 organized crime is involved;



1 (2) There is probable cause [~~for belief~~] to believe that  
2 particular communications concerning that offense will  
3 be obtained through [~~such~~] the interception;

4 (3) Normal investigative procedures have been tried and  
5 have failed or reasonably appear to be either unlikely  
6 to succeed if tried or to be too dangerous; and

7 (4) There is probable cause [~~for belief~~] to believe that  
8 the facilities from which, or the place where, the  
9 wire, oral, or electronic communications are to be  
10 intercepted are being used, or are about to be used,  
11 in connection with the commission of such offense, or  
12 are leased to, listed in the name of, or commonly used  
13 by [~~such~~] that person.

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

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

19 (1) The identity or description of all persons, if known,  
20 whose communications are to be intercepted;

21 (2) The nature and location of the communications  
22 facilities as to which, or the place where, authority



1 to intercept is granted, and the means by which such  
2 interceptions shall be made;

3 (3) A particular description of the type of communication  
4 sought to be intercepted, and a statement of the  
5 particular offense to which it relates;

6 (4) The identity of the agency authorized to intercept the  
7 communications and the persons applying for the  
8 application;

9 (5) The period of time during which [~~such~~] the  
10 interception is authorized, including a statement as  
11 to whether or not the interception [~~shall~~  
12 ~~automatically~~] is to terminate automatically [~~when~~]  
13 upon the described communication [~~has been~~] first  
14 being obtained; and

15 (6) How the authorization is to be accomplished.

16 Upon request of the applicant, [An] an order authorizing the  
17 interception of a wire, oral, or electronic communication shall  
18 [~~upon request of the applicant,~~] direct that a provider of  
19 wire or electronic communication service, landlord, custodian,  
20 or other person shall furnish the applicant [~~forthwith~~] as soon  
21 as practicable all information, facilities, and technical  
22 assistance necessary to accomplish the interception



1 unobtrusively and with a minimum of interference with the  
2 services that [~~such~~] the provider of wire or electronic  
3 communication service, landlord, custodian, or other person is  
4 according the person whose communications are to be intercepted.  
5 Any provider of wire or electronic communication service,  
6 landlord, custodian, or other person furnishing [~~such~~] the  
7 facilities or technical assistance shall be compensated  
8 [~~therefor~~] by the applicant [~~at the prevailing rates~~] for  
9 reasonable expenses incurred in providing the facilities or  
10 assistance.

11 (e) No order entered under this section shall authorize or  
12 approve the interception of any wire, oral, or electronic  
13 communication for any period longer than is necessary to achieve  
14 the objective of the authorization, [~~nor~~] and in [~~any~~] no event  
15 for longer than thirty days. The thirty-day period begins on  
16 the earlier of the day on which the investigative or law  
17 enforcement officer first begins to conduct an interception  
18 under the order or ten days after the order is entered.  
19 Extensions of an order may be granted, but only upon application  
20 for an extension made in accordance with subsections (a) and (b)  
21 of this section and the court making the findings required by  
22 subsection (c) of this section. The period of extension shall



1 be no longer than the [~~authorizing circuit court~~] designated  
2 judge deems necessary to achieve the purposes for which it was  
3 granted and in no event for longer than fifteen days. Every  
4 order and extension thereof shall contain a provision that the  
5 authorization to intercept shall be executed as soon as  
6 practicable, shall be conducted in such a way as to minimize the  
7 interception of communications not otherwise subject to  
8 interception under this part, and shall terminate upon  
9 attainment of the authorized objective, or in any event in  
10 thirty days or in fifteen days in case of an extension. [~~In the~~  
11 ~~event~~] If the intercepted communication is in a code or a  
12 foreign language, and an expert in that foreign language or code  
13 is not reasonably available during the interception period,  
14 minimization may be accomplished as soon as practicable after  
15 [~~such~~] the interception.

16 An interception may be conducted in whole or in part by  
17 investigative or law enforcement officer(s), or by an individual  
18 operating under a contract with the State or a county, acting  
19 under the supervision of an investigative or law enforcement  
20 officer authorized to conduct the interception.

21 (1) The interception shall be conducted in such a way as  
22 to minimize the resulting invasion of privacy





1 including but not limited to the following methods of  
2 minimization:

3 (A) Conversations that appear unlikely to result in  
4 incriminating conversations relating to the  
5 offense for which the order is issued shall be  
6 subject to intermittent monitoring; and

7 (B) Privileged conversations, including those between  
8 a person and the person's spouse, attorney,  
9 physician, or clergy, shall not be intercepted  
10 unless both parties to the conversation are named  
11 or described in the application and order.

12 (2) In determining whether incriminating statements are  
13 likely to occur during a conversation the following  
14 factors should be considered:

15 (A) The parties to the conversation;

16 (B) The particular offense being investigated;

17 (C) The subject matter of the conversation;

18 (D) The subject matter of previous conversations  
19 between the same parties and whether any  
20 incriminating statements occurred; and

21 (E) The hour and day of conversation.



1 (f) Whenever an order authorizing interception is entered  
2 pursuant to this part, the order shall require reports to be  
3 made to the [~~court which~~] designated judge who issued the order  
4 showing what progress has been made toward achievement of the  
5 authorized objective and the need for continued interception.  
6 [~~Such~~] The reports shall be made at such intervals as the  
7 [~~court~~] designated judge may require.

8 (g) (1) The contents of any wire, oral, or electronic  
9 communication intercepted by any means authorized by  
10 this part shall, if possible, be recorded on tape or  
11 wire or other comparable device. The recording of the  
12 contents of any wire, oral, or electronic  
13 communication under this subsection shall be done [~~in~~  
14 ~~such way as will~~] to protect the recording from  
15 [~~editing~~] being edited or [~~other alterations~~]  
16 otherwise altered. Immediately upon the expiration of  
17 the time period [~~of~~] provided in the order, or  
18 extensions thereof, [~~such recordings~~] the recording  
19 shall be made available to the [~~court~~] designated  
20 judge issuing [~~such~~] the order and sealed under the  
21 [~~court's~~] designated judge's directions. Custody of  
22 the [~~recordings~~] recording shall be [~~wherever the~~



1 ~~court orders]~~ determined by order of the designated  
2 judge. Recordings and other evidence of the contents  
3 of conversations and applications and orders shall not  
4 be destroyed except upon an order of the [~~issuing or~~  
5 ~~denying court]~~ designated judge and in any event shall  
6 be kept for ten years. However, upon the request of  
7 all the parties to particular conversations, evidence  
8 of conversations between those parties shall be  
9 destroyed (A) if there are no incriminating  
10 statements; (B) if any incriminating statements relate  
11 to only misdemeanor offenses; or (C) if the  
12 interception of the conversations is determined to  
13 have been illegal. Duplicate recordings may be made  
14 for use or disclosure pursuant to section 803-45(a)  
15 and (b) for investigations. The presence of the seal  
16 [~~provided for]~~ required by this subsection, or a  
17 satisfactory explanation for the absence thereof,  
18 shall be a prerequisite for the use or disclosure of  
19 the contents of any wire, oral, or electronic  
20 communication or evidence derived therefrom under  
21 section 803-45(c).



- 1           (2) Applications made and orders granted under this part,  
2           ~~[transcripts of hearings on applications,~~] and  
3           evidence obtained through court-ordered interceptions  
4           shall be sealed by the designated ~~[circuit court]~~  
5           judge. Custody of the above shall be ~~[whenever]~~  
6           wherever the ~~[court]~~ designated judge directs.  
7           Applications and orders shall be disclosed only upon a  
8           showing of good cause before a designated judge and  
9           shall not be destroyed, except upon order of the  
10           designated judge, and, in any event, shall be kept for  
11           ten years.
- 12           (3) Any violation of the provisions of this subsection may  
13           be punished as contempt ~~[of]~~ by the ~~[issuing or~~  
14           ~~denying court]~~ designated judge.
- 15           (4) Within a reasonable time but no later than ninety days  
16           after the termination of the period of an order or  
17           extensions thereof, the ~~[issuing court]~~ designated  
18           judge shall cause an inventory to be served~~[,]~~ on the  
19           persons named in the order, on all other known parties  
20           to intercepted communications, and to ~~[such]~~ any other  
21           persons as the court may determine is in the interest



1 of justice~~[, an]~~. The inventory ~~[which]~~ shall include  
2 notice of:

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

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

6 (C) The fact ~~[whether]~~ that during the applicable  
7 time period, wire, oral, or electronic  
8 communications were or were not intercepted; and

9 (D) The fact ~~[whether]~~ that any incriminating  
10 statements were or were not intercepted.

11 The designated ~~[circuit court]~~ judge, upon the filing  
12 of a motion, shall make available to ~~[such]~~ the person  
13 or the person's counsel for inspection after the  
14 inventory has been served all portions of the  
15 intercepted communications ~~[which]~~ that contain  
16 conversations of that person, applications, orders,  
17 ~~[transcripts of hearing,]~~ and other evidence obtained  
18 as a result of the use of interception orders. The  
19 ~~[court]~~ designated judge may order ~~[such]~~ the  
20 additional disclosure as the ~~[court]~~ designated judge  
21 determines to be in the interest of justice. On an ex  
22 parte showing of good cause, ~~[to a court]~~ the



1           designated judge may permit the serving of the  
2           inventory required by this subsection [~~may~~] to be  
3           postponed.

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

16          (i) (1) Any aggrieved person in any trial, hearing, or  
17          proceeding in or before any court, department,  
18          officer, agency, regulatory body, or other authority  
19          of this State, or a political subdivision thereof, may  
20          move to suppress the content of any intercepted wire,  
21          oral, or electronic communication, or evidence derived  
22          therefrom, on the grounds that:



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

7 Such motion shall be made before the trial, hearing,

8 or proceedings unless there was no opportunity to make

9 such motion or the person was not aware of the grounds

10 of the motion. If the motion is granted, the contents

11 of the intercepted wire, oral, or electronic

12 communication, or evidence derived therefrom, shall be

13 treated as having been obtained in violation of this

14 part. The court, or other official before whom the

15 motion is made, upon the filing of [~~such~~] the motion

16 by the aggrieved person, shall make available to the

17 aggrieved person or the aggrieved person's counsel for

18 inspection portions of the recording [~~which~~] that

19 contain intercepted communications of the defendant or

20 evidence derived therefrom, the applications, orders,

21 transcript of hearing, and such additional evidence as

22 the court determines to be in the interest of justice.



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

3 (A) From an order granting a motion to suppress made  
4 under paragraph (1) of this subsection if the  
5 attorney general or prosecuting attorney of a  
6 county, or their designated representatives,  
7 shall certify to the [~~court~~] designated judge or  
8 other official granting [~~such~~] the motion that  
9 the appeal shall be taken within thirty days  
10 after the date the order of suppression was  
11 entered and shall be diligently prosecuted as in  
12 the case of other interlocutory appeals or under  
13 such rules as the supreme court may adopt;

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

19 **§803-47 Reports concerning intercepted wire, oral, or**  
20 **electronic communications; reports concerning pen registers and**  
21 **trap and trace devices.** (a) In January of each year, the  
22 attorney general and county prosecuting attorneys of this State





1 shall report to the administrative director of the courts of  
2 this State and to the administrative office of the United States  
3 Courts:

4 (1) The fact that an order or extension was applied for;

5 (2) The kind of order or extension applied for;

6 (3) The fact that the order or extension was granted as  
7 applied for, was modified, or was denied;

8 (4) The period of interceptions authorized by the order,  
9 and the number and duration of any extensions of the  
10 order;

11 (5) The offense specified in the order or application, or  
12 extension of an order;

13 (6) The identity of the investigative or law enforcement  
14 officer and agency requesting the application and the  
15 person authorizing the request for application;

16 (7) The nature of the facilities from which or the place  
17 where communications were to be intercepted;

18 (8) A general description of the interceptions made under  
19 such order or extension, including:

20 (A) [~~the~~] The approximate nature and frequency of  
21 incriminating communications intercepted[τ];



- 1 (B) [~~the~~] The approximate nature and frequency of  
2 other communications intercepted[~~τ~~];
- 3 (C) [~~the~~] The approximate number of persons whose  
4 communications were intercepted[~~τ~~]; and
- 5 (D) [~~the~~] The approximate nature, amount, and cost of  
6 the [~~manpower~~] personnel and other resources used  
7 in the interceptions;
- 8 (9) The number of arrests resulting from interceptions  
9 made under [~~such~~] an order or extension of the order,  
10 and the offenses for which the arrests were made;
- 11 (10) The number of trials resulting from [~~such~~] the  
12 interceptions;
- 13 (11) The number of motions to suppress made with respect to  
14 [~~such~~] the interceptions[~~τ~~] and the number granted or  
15 denied;
- 16 (12) The number of convictions resulting from [~~such~~] the  
17 interceptions and the offenses for which the  
18 convictions were obtained and a general assessment of  
19 the importance of the interceptions;
- 20 (13) The information required by paragraphs (2) through (6)  
21 of this subsection with respect to orders or



1 extensions obtained in a preceding calendar year and  
2 not yet reported; and

3 (14) Other information required by the rules and  
4 regulations of the administrative office of the United  
5 States Courts.

6 (b) In March of each year the administrative director of  
7 the courts shall transmit to the legislature a full and complete  
8 report concerning the number of applications for orders  
9 authorizing or approving the interception of wire, oral, or  
10 electronic communications and the number of orders and  
11 extensions granted or denied during the preceding calendar year.  
12 [~~Such~~] The report shall include a summary and analysis of the  
13 data required to be filed with the administrative director of  
14 the courts by the attorney general and prosecuting attorneys.

15 (c) The attorney general, at least twenty days prior to  
16 the convening of each regular session, shall annually report to  
17 the legislature on the number of pen register orders and orders  
18 for trap and trace devices applied for by law enforcement  
19 agencies of the State.

20 **[\$803-47.5] Disclosure of contents of communication while**  
21 **in electronic storage.**



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

6 (2) A person or entity providing remote computing  
7 [~~services~~] service to the public shall not knowingly  
8 divulge to any person or entity the contents of any  
9 communication [~~which~~] that is carried or maintained on  
10 that service:

11 (A) On behalf of, and is either received by means of  
12 computer processing of communications or by  
13 electronic transmission, from [~~or created by~~  
14 ~~means of computer processing of communications~~  
15 ~~received by means of electronic transmissions~~  
16 ~~from~~] a subscriber or customer of [~~such~~] the  
17 service; and

18 (B) Solely for the purpose of providing storage [~~and~~]  
19 or computer processing services to [~~such~~] the  
20 subscriber or customer, if the provider is not  
21 authorized to access the contents of [~~any such~~]  
22 those communications for purposes of providing



1                   any services other than storage or computer  
2                   processing.

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

5           (1) To an addressee~~[,]~~ or intended recipient of the  
6           communication~~[,]~~ or ~~[the]~~ an agent of the  
7           ~~[addressee's]~~ addressee or intended ~~[recipient's~~  
8           ~~agent, of such communication]~~ recipient;

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

11           (3) With the lawful consent of the originator, addressee,  
12           or intended recipient of ~~[such]~~ the communication, or  
13           the subscriber in the case of a remote computing  
14           service;

15           (4) To a person employed or authorized or whose facilities  
16           are used to forward ~~[such]~~ the communication to its  
17           destination;

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

21           (6) To a law enforcement agency, if ~~[such]~~ the contents:



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

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

4 **§803-47.6 Requirements for governmental access.** (a) A  
5 governmental entity may require the disclosure by a provider of  
6 electronic communication service of the contents of an  
7 electronic communication that has been in electronic storage for  
8 one hundred and eighty days~~[7]~~ or less, [~~from the provider of~~  
9 ~~the electronic communication service~~] where storage has taken  
10 place, [~~only by means of~~] pursuant to a search warrant only. A  
11 governmental entity may require the disclosure by a provider of  
12 electronic communication service of the contents of an  
13 electronic communication [~~which~~] that has been in electronic  
14 storage for more than one hundred and eighty days by the means  
15 available under subsection (b) of this section.

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

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



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

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

8           (1) On behalf of, and received by electronic transmission  
9           from (or created by computer processing of  
10           communications received by electronic transmission  
11           from), a subscriber or customer of [~~such~~] the remote  
12           computing service; and

13           (2) Solely for the purpose of providing storage or  
14           computer processing services to [~~such~~] the subscriber  
15           or customer, if the provider is not authorized to  
16           access the contents of [~~any such~~] those communications  
17           for any purpose other than storage or computer  
18           processing.

19           (d) (1) A provider of electronic communication service or  
20           remote computing [~~services~~] service may disclose a  
21           record or other information pertaining to a subscriber  
22           to, or customer of, [~~such~~] the service (other than the



1 contents of any electronic communication) to any  
2 person other than a governmental entity.

3 (2) A provider of electronic communication service or  
4 remote computing [~~services~~] service shall disclose a  
5 record or other information pertaining to a subscriber  
6 to, or customer of, [~~such~~] the service (other than the  
7 contents of an electronic communication) to a  
8 governmental entity only when:

9 (A) Presented with a search warrant;

10 (B) Presented with a court order for [~~such~~] the  
11 disclosure;

12 (C) The consent of the subscriber or customer to  
13 [~~such~~] the disclosure has been obtained; or

14 (D) Presented with an administrative subpoena [~~issued~~  
15 ~~pursuant to section 28-2.5~~] authorized by  
16 statute, an attorney general subpoena, or a grand  
17 jury or trial subpoena, which seeks the  
18 disclosure of information concerning electronic  
19 communication, including but not limited to the  
20 name, address, local and long distance telephone  
21 [~~te~~] billing records, telephone number or other  
22 subscriber number or identity, and length of





1 service of a subscriber to or customer of the  
2 service, and the types of [~~service utilized by~~]  
3 services the subscriber or customer utilized.

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

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

18 (f) No cause of action shall lie in any court against any  
19 provider of wire or electronic communication service, its  
20 officers, employees, agents, or other specified persons for  
21 providing information, facilities, or assistance in accordance  
22 with the terms of a court order, warrant, or subpoena.



1           **[§803-47.7] Backup preservation.** (a) A governmental  
2 entity may include in its court order a requirement that the  
3 service provider create a backup copy of the contents of the  
4 electronic communication without notifying the subscriber or  
5 customer. The service provider shall create [~~such~~] the backup  
6 copy as soon as practicable, consistent with its regular  
7 business practices, and shall confirm to the governmental entity  
8 that [~~such a~~] the backup copy has been made. [~~Such~~] The backup  
9 copy shall be created within two business days after receipt by  
10 the service provider of [a] the subpoena or court order [~~by the~~  
11 ~~service provider~~].

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

16           (c) The service provider shall not destroy [~~such~~] the  
17 backup copy until the later of:

- 18           (1) The delivery of the information; or  
19           (2) The resolution of any proceedings, including any  
20           appeal therefrom, concerning a court order.

21           (d) The service provider shall release [~~such~~] the backup  
22 copy to the requesting governmental entity no sooner than



1 fourteen days after the governmental entity's notice to the  
2 subscriber or customer, if [~~such~~] the service provider:

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

6 (2) Has not initiated proceedings to challenge the  
7 [~~governmental entity's~~] request of the governmental  
8 entity.

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

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



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

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

15          (g) If the court finds that the applicant is not the  
16          subscriber or customer whose communications are sought, or that  
17          there is reason to believe that the law enforcement inquiry is  
18          legitimate and the justification for the communications sought  
19          is supported by probable cause, the application or motion shall  
20          be denied, and the court shall order the release of the backup  
21          copy to the government entity. A court order denying a motion  
22          or application shall not be deemed a final order, and no



1 interlocutory appeal may be taken therefrom by the customer. If  
2 the court finds that the applicant is a proper subscriber or  
3 customer and the justification for the communication sought is  
4 not supported by probable cause or that there has not been  
5 substantial compliance with the provisions of this part, it  
6 shall order vacation of the order previously issued.

7 **[\$803-47.8] Delay of notification.** (a) A governmental  
8 entity may as part of a request for a court order include a  
9 provision that notification be delayed for a period not  
10 exceeding ninety days if the court determines that notification  
11 of the existence of the court order may have an adverse result.

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

- 14 (1) Endangering the life or physical safety of an  
15 individual;
- 16 (2) Flight from prosecution;
- 17 (3) Destruction of or tampering with evidence;
- 18 (4) Intimidation of a potential witness; or
- 19 (5) Otherwise seriously jeopardizing an investigation or  
20 unduly delaying a trial.



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

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

8 (1) States with reasonable specificity the nature of the  
9 law enforcement inquiry; and

10 (2) Informs [~~such~~] the customer or subscriber:

11 (A) [~~That information~~] Information maintained for  
12 [~~such~~] the customer or subscriber by the service  
13 provider or request was supplied to or requested  
14 by that governmental authority and the date on  
15 which the supplying or request took place;

16 (B) [~~That notification~~] Notification of [~~such~~] the  
17 customer or subscriber was delayed;

18 (C) [~~What~~] The governmental entity or court that made  
19 the certification or determination upon which the  
20 delay was made; and

21 (D) [~~Which~~] The provision of this part that allowed  
22 [~~such~~] the delay.



1           (e) A governmental entity may apply to the [~~circuit court~~]  
2 designated judge [~~by the chief justice of the Hawaii supreme~~  
3 ~~court~~] or any other circuit judge or district court judge, if a  
4 circuit court judge has not yet been designated by the chief  
5 justice of the Hawaii supreme court, or is otherwise  
6 unavailable, for an order commanding a provider of an electronic  
7 communication service or remote computing service to whom a  
8 search warrant, or court order is directed, not to notify any  
9 other person of the existence of the search warrant, or court  
10 order for such period as the court deems appropriate not to  
11 exceed ninety days. The court shall enter [~~such an~~] the order  
12 if it determines that there is reason to believe that  
13 notification of the existence of the search warrant, or court  
14 order will result in:

- 15           (1) Endangering the life or physical safety of an  
16                 individual;
- 17           (2) Flight from prosecution;
- 18           (3) Destruction of or tampering with evidence;
- 19           (4) Intimidation of [~~a~~] potential [~~witness~~] witnesses; or
- 20           (5) Otherwise seriously jeopardizing an investigation or  
21                 unduly delaying a trial.



1            **[§803-47.9] Cost reimbursement.** (a) A government entity  
2 obtaining the contents of communications, records, or other  
3 information shall ~~reimburse any~~ pay to the person or entity  
4 ~~[reasonable fees for]~~ providing or assembling [such] the  
5 information a fee for reimbursement or costs that are reasonably  
6 necessary and that have been directly incurred in searching for,  
7 assembling, reproducing, or otherwise providing the information.  
8 ~~[Such]~~ The reimbursable costs shall include any costs due to  
9 necessary disruption of normal operations of any electronic  
10 communication service or remote computing service ~~[which]~~ that  
11 was occasioned by the governmental needs.

12            (b) The amount of the fee provided by subsection (a) shall  
13 be as mutually agreed by the governmental entity and the person  
14 or entity providing the information or, in the absence of  
15 agreement, shall be as determined by the designated court that  
16 issued the order for production of the information or the court  
17 before which a criminal prosecution relating to the information  
18 would be brought, if no court order was issued for production of  
19 the information.

20            (c) The requirement of subsection (a) does not apply with  
21 respect to records or other information maintained by a  
22 communication common carrier that relate to telephone toll





1 records and telephone listings obtained under section 803-47.6.  
2 However, the court may order a payment as described in  
3 subsection (a), if the court determines the information required  
4 is unusually voluminous in nature or otherwise caused an undue  
5 burden on the provider.

6       **§803-48 Recovery of civil damages authorized.** Any person  
7 whose wire, oral, or electronic communication is accessed,  
8 intercepted, disclosed, or used in violation of this part shall  
9 (1) have a civil cause of action against any person who  
10 accesses, intercepts, discloses, or uses, or procures any other  
11 person to access, intercept, disclose, or use [~~such~~] the  
12 communications, and (2) be entitled to recover from any such  
13 person:

- 14       (A) The greater of (i) the sum of the actual damages  
15           suffered by the plaintiff and any profits made by the  
16           violator as a result of the violation, or (ii)  
17           statutory damages of [~~whichever is~~] the greater of  
18           \$100 a day for each day of violation or \$10,000;
- 19       (B) Punitive damages, where appropriate; and
- 20       (C) A reasonable attorney's fee and other litigation costs  
21           reasonably incurred.



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

6 **§803-48.5 Injunction against illegal interception.**

7 Whenever it appears that any person is engaged or is about to  
8 engage in any act that constitutes or will constitute a felony  
9 violation of this part, the attorney general may initiate a  
10 civil action in a circuit court of this State to enjoin the  
11 violation. The court shall proceed as soon as practicable to  
12 the hearing and make a determination of the action; provided  
13 that at any time before final determination, the court may enter  
14 a restraining order or take any other action that is warranted  
15 to prevent a continuing and substantial injury to the State or  
16 to any person or class of persons for whose protection the  
17 action is brought. A proceeding under this section is governed  
18 by the Hawaii rules of civil procedure; except that, if an  
19 indictment, information, or criminal complaint has been returned  
20 against the respondent, discovery shall be governed by the  
21 Hawaii rules of penal procedure.



1           **§803-49 Severability.** If any portion or subsection of  
2 this part or the application thereof to any person or  
3 circumstances is invalid, such invalidity shall not affect other  
4 sections or applications of the part which can be given effect  
5 without the invalid section or application, and to this end the  
6 provisions of this part are declared to be severable.

7           **§803-50 REPEALED.** L 1984, c 91, §1."

8           SECTION 3. This Act does not affect rights and duties that  
9 matured, penalties that were incurred, and proceedings that were  
10 begun, before its effective date.

11           SECTION 4. Statutory material to be repealed is bracketed  
12 and stricken. New statutory material is underscored.

13           SECTION 5. This Act shall take effect on July 1, 2050.

