

---

# 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  
2 by adding a new section to be appropriately designated and to  
3 read 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, is amended by adding a  
5 new section to be appropriately designated and to read as  
6 follows:

7 **"§803-48.5 Injunction against illegal interception.**

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



1 SECTION 3. Section 641-13, Hawaii Revised Statutes, is  
2 amended to read as follows:

3 **"§641-13 By State in criminal cases.** An appeal may be  
4 taken by and on behalf of the State from the district or circuit  
5 courts to the supreme appellate court, subject to chapter 602,  
6 in all criminal [~~eases~~] matters, in the following instances:

- 7 (1) From an order or judgment quashing, setting aside, or  
8 sustaining a motion to dismiss[~~τ~~] any indictment,  
9 information, or complaint or any count thereof;
- 10 (2) From an order or judgment[~~τ~~] sustaining a special plea  
11 in bar[~~τ~~] or dismissing the case where the defendant  
12 has not been put in jeopardy;
- 13 (3) From an order granting a new trial;
- 14 (4) From an order arresting judgment;
- 15 (5) From a ruling on a question of law adverse to the  
16 State, where the defendant was convicted and appeals  
17 from the judgment;
- 18 (6) From the sentence, on the ground that it is illegal;
- 19 (7) From a pretrial order granting a motion for the  
20 suppression of evidence, including a confession or  
21 admission, or the return of property, in which case  
22 the intermediate appellate court or the supreme court,



1 as the case may be, shall give priority to [~~such an~~  
2 the appeal and the order shall be stayed pending the  
3 outcome of the appeal;

4 (8) From an order denying a request by the State for  
5 protective order for nondisclosure of witness for  
6 [~~their~~] reason of personal safety under Rule 16(e) (4)  
7 of the Hawaii Rules of Penal Procedure, in which case  
8 the intermediate appellate court shall give priority  
9 to [~~such~~] the appeal and the order shall be stayed  
10 pending outcome of [~~such~~] the appeal; [~~or~~]

11 (9) From a judgment of acquittal following a jury verdict  
12 of guilty[~~-~~]; and

13 (10) From a denial of an application for an order of  
14 approval or authorization of the interception of a  
15 wire, oral, or electronic communication pursuant to  
16 section 803-44."

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

19 "PART IV. ELECTRONIC EAVESDROPPING

20 §803-41 Definitions. As used in [~~It~~] this part, unless  
21 the context clearly requires otherwise:

1 "Aggrieved person" means a person who was party to any  
2 intercepted wire, oral, or electronic communication or a person  
3 against whom the interception was directed.

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

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

10 [~~"Aural transfer" means a transfer containing the human~~  
11 ~~voice at any point between and including the point of origin and~~  
12 ~~the point of reception.]~~

13 "Communication common carrier" means any person engaged as  
14 a common carrier for hire in interstate or foreign communication  
15 by wire or radio or in intrastate, interstate, or foreign radio  
16 transmission of energy, except where reference is made to  
17 communication common carriers not subject to this part; provided  
18 that a person engaged in radio broadcasting, to the extent the  
19 person is so engaged, shall not be deemed a communication common  
20 carrier.



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

4 "Designated judge" means a circuit court judge designated  
5 by the chief justice of the Hawaii supreme court to issue orders  
6 under this part.

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

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

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

19 [~~(3)] (2) Any communication made through a tone-only paging~~  
20 ~~device; [~~or~~]~~

21 [~~(4)] (3) Any communication from a tracking device [~~-~~]; or~~



1       (4) Electronic funds transfer information stored by  
2           financial institution in a communications system used  
3           for the electronic storage and transfer of funds.

4       "Electronic communication service" means any service that  
5 provides to users thereof the ability to send or receive wire or  
6 electronic communications.

7       "Electronic communication system" means any wire, radio,  
8 electromagnetic, [~~photooptical~~] photo-optical, or  
9 photoelectronic facilities for the transmission of electronic  
10 communications, and any computer facilities or related  
11 electronic equipment for the electronic storage of [~~such~~] these  
12 communications.

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

16       (1) Any telephone or telegraph instrument, equipment or  
17 facility, or any component thereof, (A) furnished to  
18 the subscriber or user by a provider of wire or  
19 electronic commu0nication service in the ordinary  
20 course of its business and being used by the  
21 subscriber or user in the ordinary course of its  
22 business or furnished by [~~such~~] the subscriber or user



1 for connection to the facilities of [~~such~~] the  
2 services and used in the ordinary course of its  
3 business; or (B) being used by a provider of wire or  
4 electronic communication service in the ordinary  
5 course of its business, or by an investigative or law  
6 enforcement officer in the ordinary course of the  
7 officer's duties; or

- 8 (2) A hearing aid or similar device being used to correct  
9 subnormal hearing to a level not better than [~~normal~~].  
10 average.

11 "Electronic storage" means:

- 12 (1) Any temporary, intermediate storage of a wire or  
13 electronic communication incidental to the electronic  
14 transmission thereof; and  
15 (2) Any storage of [~~such~~] the communication by an  
16 electronic communication service for purposes of  
17 backup protection of [~~such~~] the communication.

18 "Intercept" means the aural or other acquisition of the  
19 contents of any wire, electronic, or oral communication through  
20 the use of any electronic, mechanical, or other device.

21 "Investigative or law enforcement officer" means any  
22 officer of the State or political subdivision thereof, who is





1 empowered by the law of this State to conduct investigations of  
2 or to make arrests for offenses enumerated in this part.

3 "Oral communication" means any [~~oral communication uttered~~]  
4 utterance by a person exhibiting an expectation that [~~such~~  
5 ~~communication~~] the utterance is not subject to interception  
6 under circumstances justifying [~~such~~] that expectation, but  
7 [~~such~~] the term does not include any electronic communication.

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

10 "Pen register" means a device [~~which~~] that records or  
11 decodes electronic or other impulses [~~which~~] that identify the  
12 numbers dialed or otherwise transmitted on the telephone line to  
13 which such device is attached, but [~~such~~] the such term does not  
14 include any device used by a provider or customer of a wire or  
15 electronic communication service for billing, or recording as an  
16 incident to billing, for communication services provided by  
17 [~~such~~] the provider or any device used by a provider or customer  
18 of a wire communication service[7] for cost accounting or other  
19 [~~like~~] similar purposes in the ordinary course of its business.

20 "Person" means any official, employee, or agent of the  
21 United States or this State or political subdivision thereof,



1 and any individual, partnership, association, joint stock  
2 company, trust, or corporation.

3 "Readily accessible to the general public" means, with  
4 respect to radio communication, that [~~such~~] the communication is  
5 not:

- 6 (1) Scrambled or encrypted;
- 7 (2) Transmitted using modulation techniques whose  
8 essential parameters have been withheld from the  
9 public with the intention of preserving the privacy of  
10 [~~such~~] the communication;
- 11 (3) Carried on a subcarrier or other signal subsidiary to  
12 a radio transmission;
- 13 (4) Transmitted over a communication system provided by a  
14 common carrier, unless the communication is a tone-  
15 only paging system communication; or
- 16 (5) Transmitted on frequencies allocated under part 25,  
17 subpart D, E, or F of part 74, or part 94 of the Rules  
18 of the Federal Communications Commission, unless in  
19 the case of a communication transmitted on a frequency  
20 allocated under part 74 that is not exclusively  
21 allocated to broadcast auxiliary services, the



1 communication is a two-way voice communication by  
2 radio.

3 "Remote computing service" means the provision to the  
4 public of computer storage or processing services by means of an  
5 electronic communication system.

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

9 (1) In a motor vehicle or other vehicle by or with the  
10 permission of the owner or person in lawful possession  
11 of the motor vehicle or other vehicle for the purpose  
12 of tracking the movement of [~~such~~] the motor vehicle  
13 or other vehicle; or

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

16 "Trap and trace device" means a device [~~which~~] that  
17 captures the incoming electronic or other impulses [~~which~~] that  
18 identify the originating number of an instrument or device from  
19 which a wire or electronic communication was transmitted.

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

21 (1) Uses an electronic communication service; and



1 (2) Is duly authorized by the provider of [~~such~~] the  
2 service to engage in such use.

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

18 **§803-42 Interception, access, and disclosure of wire,**  
19 **oral, or electronic communications, use of pen register, trap**  
20 **and trace device, and mobile tracking device prohibited. (a)**

21 Except as otherwise specifically provided in this part, any  
22 person who:



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

5 (2) Intentionally uses, endeavors to use, or procures any  
6 other person to use or endeavor to use any electronic,  
7 mechanical, or other device to intercept any wire,  
8 oral, or electronic communication[+] when:

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

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

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

1 (4) Intentionally uses, or endeavors to use, the contents  
2 of any wire, oral, or electronic communication,  
3 knowing or having reason to know that the information  
4 was obtained through the interception of a wire, oral,  
5 or electronic communication in violation of this part;

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

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

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

19 (A) Either:

20 (i) Knowing or having reason to know that the  
21 information was obtained through the

1 interception of the communication in  
2 connection with a criminal investigation; or

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

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

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

12 [+7+] (8) Intentionally installs or uses a mobile tracking  
13 device without first obtaining a search warrant or  
14 other order authorizing the installation and use of  
15 such device[+], unless the device is installed by or  
16 with consent of the owner of the property on which the  
17 device is installed;

18 shall be guilty of a class C felony.

19 (b) (1) It shall not be unlawful under this part for an  
20 operator of a switchboard, or an officer, employee, or  
21 agent of a provider of wire or electronic  
22 communication services, whose facilities are used in



1 the transmission of a wire communication, to  
2 intercept, disclose, or use that communication in the  
3 normal course of the officer's, employee's, or agent's  
4 employment while engaged in any activity [~~which~~] that  
5 is either a necessary incident to the rendition of the  
6 officer's, employee's, or agent's service or to the  
7 protection of the rights or property of the provider  
8 of that service; provided that [~~such~~] providers of  
9 wire communication service to the public shall not  
10 utilize service observing or random monitoring except  
11 for mechanical or service quality control checks.

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





1           (3) (A) It shall not be unlawful under this part for a  
2           person not acting under color of law to intercept a  
3           wire, oral, or electronic communication [~~where such~~]  
4           when the person is a party to the communication or  
5           [~~where~~] when one of the parties to the communication  
6           has given prior consent to [~~such~~] the interception  
7           unless [~~such~~] the communication is intercepted for the  
8           purpose of committing any criminal or tortious act in  
9           violation of the Constitution or laws of the United  
10          States or of this State [~~; provided that installation~~].

11          (B) It shall not be unlawful for a person acting  
12          under color of law to install in any private place,  
13          without consent of the person or persons entitled to  
14          privacy therein, [~~of~~] any device for recording,  
15          amplifying, or broadcasting sounds or events in that  
16          place, or use of any such unauthorized installation,  
17          or installation or use outside a private place of such  
18          device to intercept sounds originating in that place  
19          which would not ordinarily be audible or  
20          comprehensible outside [~~; without the consent of the~~  
21          ~~person or persons entitled to privacy therein is~~  
22          ~~prohibited~~].



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

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

19 (6) Notwithstanding any other law[~~7~~] to the contrary,  
20 providers of wire or electronic communication service,  
21 their officers, employees, and agents, landlords,  
22 custodians, or other persons, are authorized to



1 provide information, facilities, or technical  
2 assistance to persons authorized by law to intercept  
3 or access wire, oral, or electronic communications, to  
4 conduct electronic surveillance, or to install a pen  
5 register or trap and trace device if such provider,  
6 its officers, employees, or agents, landlord,  
7 custodian, or other specified person, has been  
8 provided with:

9 (A) A court order directing such assistance signed by

10 [~~an authorizing~~] the designated judge; or

11 (B) A certification in writing from the Attorney

12 General of the United States, the Deputy Attorney

13 General of the United States, the Associate

14 Attorney General of the United States, the

15 attorney general of the State of Hawaii, or the

16 prosecuting attorney for each county that no

17 warrant or court order is required by law, that

18 all statutory requirements have been met, and

19 that the specific assistance is required, setting

20 forth the period of time during which the

21 providing of the information, facilities, or

22 technical assistance is authorized and specifying



1 the information, facilities, or technical  
2 assistance required.

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

15 No cause of action shall lie in any court  
16 against any provider of wire or electronic  
17 communication service, its officers, employees,  
18 or agents, landlord, custodian, or other  
19 specified person for providing information,  
20 facilities, or assistance in accordance with the  
21 terms of a court order or certification under  
22 this part.



- 1 (7) It shall not be unlawful under this part for any  
2 person:
- 3 (A) To intercept or access an electronic  
4 communication made through an electronic  
5 communication system configured so that [~~such~~]  
6 the electronic communication is readily  
7 accessible to the general public.
- 8 (B) To intercept any radio communication [~~which~~] that  
9 is transmitted:
- 10 (i) By any station for the use of the general  
11 public, or that relates to ships, aircraft,  
12 vehicles, or persons in distress;
- 13 (ii) By any governmental, law enforcement, civil  
14 defense, private land mobile, or public  
15 safety communications system, including  
16 police and fire, readily accessible to the  
17 general public;
- 18 (iii) By a station operating on an authorized  
19 frequency within the bands allocated to the  
20 amateur, citizens band, or general mobile  
21 radio services; or



1 (iv) By any marine or aeronautical communications  
2 system.

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

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

7 (ii) Is excepted from the application of section  
8 705(a) of the Communications Act of 1934 by  
9 section 705(b) of that Act (47 U.S.C. §605).

10 (D) To intercept any wire or electronic communication  
11 the transmission of which is causing harmful  
12 interference to any lawfully operating station or  
13 consumer electronic equipment to the extent  
14 necessary to identify the source of [~~such~~] the  
15 interference;

16 (E) For other users of the same frequency to  
17 intercept any radio communication made through a  
18 system that uses frequencies monitored by  
19 individuals engaged in the providing or the use  
20 of [~~such~~] the system, if [~~such~~] the communication  
21 is not scrambled or encrypted.

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



- 1 (A) To use a pen register or a trap and trace device  
2 as specified in this part.
- 3 (B) For a provider of electronic communication  
4 service to record the fact that a wire or  
5 electronic communication was initiated or  
6 completed in order to protect [~~such~~] the  
7 provider, another provider furnishing service  
8 toward the completion of the wire or electronic  
9 communication, or a user of that service, from  
10 the fraudulent, unlawful, or abusive use of such  
11 service.
- 12 (C) For a provider of electronic or wire  
13 communication service to use a pen register or a  
14 trap and trace device for purposes relating to  
15 the operation, maintenance, and testing of the  
16 wire or electronic communication service or to  
17 the protection of the rights or property of  
18 [~~such~~] the provider, or to the protection of  
19 users of that service from abuse of service or  
20 unlawful use of service.



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

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

7 (10) Except as provided in this section, a person or entity  
8 providing an electronic communication service to the  
9 public shall not intentionally divulge the contents of  
10 any communication (other than a communication to the  
11 person or entity or an agent thereof) while in  
12 transmission on that service to any person or entity  
13 other than an addressee or intended recipient of the  
14 communication or an agent of the addressee or intended  
15 recipient.

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

19 (A) As otherwise authorized by a court order[+] or  
20 under this part;





1 (B) With the lawful consent of the originator,  
2 addressee, [~~originator~~] or intended recipient[~~+~~]  
3 of the communication;

4 (C) To a person employed or authorized, or whose  
5 facilities are used, to forward [~~such~~] the  
6 communication to its destination; or

7 (D) [~~Which were~~] That was inadvertently obtained by  
8 the service provider and [~~which appear~~] that  
9 appears to pertain to the commission of a crime,  
10 if divulged to a law enforcement agency.

11 **§803-43 Devices to intercept wire, oral, or electronic**  
12 **communications and advertising of same prohibited; penalty;**  
13 **forfeiture.** Any person, other than a provider of wire or  
14 electronic communication service and its duly authorized  
15 officers, employees, and agents, or any person acting under  
16 color of law, who, in this State, intentionally manufactures,  
17 assembles, possesses, or distributes, or who attempts to  
18 distribute, any electronic, mechanical, or other device, knowing  
19 or having reason to know that the device or the design of the  
20 device renders it primarily useful for the purpose of  
21 surreptitious interception of wire, oral, or electronic  
22 communications, or who intentionally places an advertisement of

1 any such device or promotes the use of any such device in any  
2 newspaper, magazine, handbill, or other publication, shall be  
3 guilty of a class C felony. Any such electronic, mechanical, or  
4 other device in violation of this section shall be subject to  
5 seizure and forfeiture under [~~title 37.~~] chapter 712A.

6       **§803-44 Application for court order to intercept wire,**  
7 **oral, or electronic communications.** The attorney general of  
8 this State, or a designated deputy attorney general in the  
9 attorney general's absence or incapacity, or the prosecuting  
10 attorney of each county, or a designated deputy prosecuting  
11 attorney in the prosecuting attorney's absence or incapacity,  
12 may make application to a [~~circuit court judge,~~] designated  
13 judge [~~by the chief justice of the Hawaii supreme court,~~] or any  
14 other circuit court judge or district court judge, if a circuit  
15 court judge has not been designated by the chief justice of the  
16 Hawaii supreme court, or is otherwise unavailable, in the county  
17 where the interception is to take place, for an order  
18 authorizing or approving the interception of wire, oral, or  
19 electronic communications, and such court may grant in  
20 conformity with section 803-46 an order authorizing, or  
21 approving the interception of wire, oral, or electronic  
22 communications by investigative or law enforcement officers



1 having responsibility for the investigation of the offense as to  
2 which the application is made, [~~when such~~] if the interception  
3 [~~may~~] might provide or has provided evidence of:

4 (a) [~~murder,~~] Murder;

5 (b) [~~kidnapping,~~] Kidnapping; [~~or~~]

6 (c) [~~felony~~] Felony criminal property damage  
7 involving the danger of [~~serious~~] bodily injury  
8 as defined in section 707-700[~~7~~];

9 (d) Distribution of dangerous, harmful, or  
10 detrimental drugs; or

11 (e) Conspiracy to commit one or more of the above;

12 or involving

13 (f) [~~organized~~] Organized crime and any of the  
14 following felony offenses:

15 (1) [~~extortion;~~] Extortion;

16 (2) [~~bribery~~] Bribery of a juror, of a witness,  
17 or of a police officer;

18 (3) [~~receiving~~] Receiving stolen property; and

19 (4) [~~gambling;~~] Gambling; and [~~distribution of~~  
20 ~~dangerous, harmful, or detrimental drugs.~~]

21 (5) Money laundering.



1           [+]§803-44.5[+]   **Application for a pen register or a trap**  
2 **and trace device.** (a) The attorney general of this State or  
3 the prosecuting attorney for each county, or a subordinate  
4 designated to act in either's absence or incapacity, may apply  
5 in writing under oath or equivalent affirmation to a [~~circuit~~  
6 ~~court judge~~] designated judge [~~by the chief justice of the~~  
7 ~~Hawaii supreme court~~] or any other circuit court judge or  
8 district court judge, if a circuit court judge has not been  
9 designated by the chief justice of the Hawaii supreme court, or  
10 is otherwise unavailable, for an order or an extension of an  
11 order to authorize the installation and use of a pen register or  
12 a trap and trace device.

13           (b) The application shall include:

14           (1) The identity of the official making the application  
15           and the law enforcement agency conducting the  
16           investigation; and

17           (2) The facts and circumstances relied upon by the  
18           applicant to conclude that there is probable cause to  
19           believe that information will be obtained through the  
20           installation and use of a pen register or trap and  
21           trace device [~~which~~] that will constitute the fruits,



1           instrumentalities, or evidence of a crime covered  
2           under this part.

3           ~~[+]~~§803-44.6~~[+]~~   **Issuance of an order for a pen register or**  
4 **a trap and trace device.** (a) Upon an application for an order  
5 authorizing the installation and use of a pen register or a trap  
6 and trace device, the ~~[reviewing]~~ designated judge shall satisfy  
7 itself that there are sufficient facts and circumstances  
8 contained within the application that there is is probable cause  
9 to believe that the information ~~[will]~~ to be obtained through  
10 the installation and use of a pen register or a trap and trace  
11 device ~~[which]~~ will constitute the fruits, instrumentalities, or  
12 evidence of a crime or is relevant to an ongoing criminal  
13 investigation.

14           (b) If the ~~[reviewing]~~ designated judge is so satisfied,  
15 the order issued shall specify:

16           (1) The identity, if known, of the person to whom is  
17           leased or in whose name is listed the telephone  
18           line to which the pen register or trap and trace  
19           device is to be attached;

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



- 1           (3) The number and, if known, the physical location  
2           of the telephone line to which the pen register  
3           or the trap and trace device is to be attached,  
4           and, in the case of a trap and trace device, the  
5           geographical limits of the trap and trace order;
- 6           (4) A statement of the offense to which the  
7           information likely to be obtained by the pen  
8           register or trap and trace device relates; and
- 9           (5) Upon the request of the applicant, the  
10          information, facilities, and technical assistance  
11          necessary to accomplish the installation of the  
12          pen register or trap and trace device that the  
13          provider of wire communication service is  
14          directed to furnish to the applicant.

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



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

3 (1) The order be sealed until otherwise ordered by the  
4 court; and

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

13 **[~~§~~§803-44.7~~]~~ Application for authorization to install**  
14 **and use a mobile tracking device.** (a) A search warrant or  
15 court order must be obtained from the [~~circuit court judge~~]  
16 designated judge [~~by the chief justice of the Hawaii supreme~~  
17 ~~court~~] or any other circuit court judge or district court judge,  
18 if a circuit court judge has not been designated by the chief  
19 justice of the Hawaii supreme court, or is otherwise  
20 unavailable, to install a mobile tracking device. [~~Such~~] The  
21 order may authorize the use of that device within the



1 jurisdiction of the court and outside that jurisdiction, if the  
2 device is installed in that jurisdiction.

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

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

12 (1) The identity, if known, of the person who is the  
13 subject of the investigation;

14 (2) The number of mobile tracking devices to be used and  
15 the geographical location(s) where the devices are to  
16 be installed; and

17 (3) The identity, if known, of any person who may have a  
18 privacy interest in the point of installation of the  
19 mobile tracking device.

20 (d) An order authorizing installation and use of a mobile  
21 tracking device shall not exceed sixty days. Extensions of  
22 [~~such~~] the orders may be granted only upon reapplication





1 establishing probable cause to justify the continued use of a  
2 mobile tracking device. The period of the extension shall not  
3 exceed sixty days.

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

6 **§803-45 Authorization for disclosure and use of**  
7 **intercepted wire, oral, or electronic communications.** (a) Any  
8 investigative or law enforcement officer, who, by any means  
9 authorized by this part, has obtained knowledge of the contents  
10 of any wire, oral, or electronic communication, or evidence  
11 derived therefrom, may disclose [~~such~~] the contents to another  
12 investigative or law enforcement officer to the extent that  
13 [~~such~~] the disclosure is appropriate to the proper performance  
14 of the official duties of the officer making or receiving the  
15 disclosure.

16 (b) Any investigative or law enforcement officer, who by  
17 any means authorized by this part, has obtained knowledge of the  
18 contents of any wire, oral, or electronic communication or  
19 evidence derived therefrom may use [~~such~~] the contents to the  
20 extent [~~such~~] the use is appropriate to the proper performance  
21 of the officer's official duties.



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

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

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



1 designated [~~circuit court~~] judge where [~~such court~~] the judge  
2 finds on subsequent application, made as soon as practicable,  
3 that the contents were otherwise intercepted in accordance with  
4 the provisions of this part.

5 (f) [~~No testimony or evidence relating to~~] Evidence  
6 obtained pursuant to an order issued under this part for the  
7 interception of a wire, oral, or electronic communication [or  
8 any evidence derived therefrom intercepted in accordance with  
9 the provisions of] pursuant to an order issued under this part  
10 shall not be admissible as evidence in the state's case in chief  
11 in a criminal case where the highest grade of offense charged is  
12 a [in support of any] misdemeanor [charge].

13 (g) No part of the contents of any wire, oral, or  
14 electronic communication and no evidence derived therefrom may  
15 be received into evidence at any trial, hearing, or other  
16 proceeding in or before any court, grand jury, department,  
17 officer, agency, regulatory body, legislative committee, or  
18 other authority of the State or a county, or be included in any  
19 information used to charge a criminal offense under chapter 806,  
20 if the disclosure would be in violation of this part.

21 **§803-46 Procedure for interception of wire, oral, or**  
22 **electronic communication.** (a) Each application for an order



1 authorizing or approving the interception of a wire, oral, or  
2 electronic communication shall be made in writing upon oath or  
3 affirmation to a designated [~~ircuit court~~] judge and shall be  
4 accompanied by a written memorandum recommending approval or  
5 disapproval by the department of attorney general. The  
6 application shall state the applicant's authority to make [~~such~~]  
7 the application. The [~~terms~~] term [~~"designated circuit,"~~]  
8 "~~designated judge~~["~~7~~"] [~~"authorized circuit court," "designated~~  
9 ~~circuit court," "issuing judge," and the "court"~~] as used in  
10 this section shall not only mean a circuit court judge  
11 specifically designated by the chief justice of Hawaii supreme  
12 court, but shall also mean any circuit court judge or district  
13 court judge if no circuit court judge has been designated by the  
14 chief justice, or is otherwise unavailable. Each application  
15 shall include the following information:

16 (1) The identity of the investigative or law enforcement  
17 officer(s) requesting the application, the official(s)  
18 applying for an order;

19 (2) A full and complete statement of the facts and  
20 circumstances relied upon by the applicant, to justify  
21 the applicant's belief that an order should be issued,  
22 including (A) details as to the particular offense



1 that has been, is being, or is about to be committed,  
2 (B) except as provided in subsection (j), a particular  
3 description of the nature and location of the  
4 facilities from which or the place where the  
5 communication is to be intercepted, (C) a particular  
6 description of the type of communications sought to be  
7 intercepted, (D) the identity or descriptions of all  
8 persons, if known, committing the offense and whose  
9 communications are to be intercepted, and where  
10 appropriate (E) the involvement of organized crime;

11 (3) A full and complete, but not unduly technical or  
12 complex, statement of the facts concerning how the  
13 interception is to be accomplished, and if physical  
14 entry upon private premises is necessary, facts  
15 supporting such necessity;

16 (4) A full and complete statement of facts as to whether  
17 or not other investigative procedures have been tried  
18 and failed or why they reasonably appear to be  
19 unlikely to succeed if tried or to be too dangerous;

20 (5) A statement of facts indicating the period of time for  
21 which the interception is required to be maintained.

22 If the nature of the investigation is such that the



1 authorization for interception should not  
2 automatically terminate when the described type of  
3 communication has been obtained, a particular  
4 description of facts establishing probable cause to  
5 believe that additional communications of the same  
6 type will occur thereafter;

7 (6) A full and complete statement of the facts concerning  
8 all previous applications known to the individual  
9 authorizing and making the application, made to any  
10 ~~[court]~~ designated judge for authorization to  
11 intercept, or for approval of interceptions of, wire,  
12 oral, or electronic communications involving any of  
13 the same persons, facilities, or places specified in  
14 the application, and the action taken by the ~~[court]~~  
15 designated judge on each ~~[such]~~ application; and

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

21 (b) ~~[An in camera adversary hearing shall be held on any~~  
22 ~~interception application or application for extension. Upon~~



1 ~~receipt of the application the designated judge shall appoint an~~  
2 ~~attorney to oppose the application. The attorney shall be~~  
3 ~~appointed and compensated in the same manner as attorneys are~~  
4 ~~appointed to represent indigent criminal defendants. The~~  
5 ~~appointed attorney shall be given at least twenty-four hours~~  
6 ~~notice of the hearing and shall be served with copies of the~~  
7 ~~application, proposed order, if any, and supporting documents~~  
8 ~~with the notice. At the hearing, the attorney appointed may~~  
9 ~~cross-examine witnesses and present arguments in opposition to~~  
10 ~~the application. The affiant supporting the application shall~~  
11 ~~be present at the hearing. If an interlocutory appeal is taken~~  
12 ~~by the State from the denial of an application, the appointed~~  
13 ~~attorney shall be retained to answer the appeal or another~~  
14 ~~attorney shall be appointed for the appeal.] The designated~~  
15 ~~[circuit court] judge~~ may require the applicant to furnish  
16 ~~[additional]~~ testimony or documentary evidence under oath or  
17 affirmation in support of the application. A transcript of the  
18 ~~[hearing]~~ testimony shall be made and kept with the application  
19 and orders.

20 (c) Upon ~~[such]~~ an application ~~[and after such adversary~~  
21 ~~hearing,]~~ the ~~[court]~~ designated judge may enter an ex parte  
22 order, as requested or as modified, authorizing or approving



1 interception of wire, oral, or electronic communications within  
2 the county in which the [~~court~~] designated judge is sitting, if  
3 the [~~court~~] designated judge determines on the basis of the  
4 facts submitted by the applicant that:

5 (1) There is probable cause [~~for belief~~] to believe that  
6 an individual is committing, has committed, or is  
7 about to commit

8 (A) [~~murder,~~] Murder;

9 (B) [~~kidnapping,~~] Kidnapping; [~~or~~]

10 (C) [~~felony~~] Felony criminal property damage  
11 involving the danger of [~~serious~~] bodily injury;

12 (D) Distribution of dangerous, harmful or detrimental  
13 drugs; or

14 (E) Conspiracy to commit one or more of the above;

15 or that an individual is committing, has committed, or  
16 is about to commit one of the other offenses specified  
17 in section 803-44 and that organized crime is  
18 involved;

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





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

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

12 If the order allows physical entry to accomplish the  
13 interception, the issuing judge shall [~~find that the~~  
14 ~~interception could not be accomplished by means other than~~]  
15 state why physical entry[-] is appropriate.

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

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

20 (2) The nature and location of the communications  
21 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. An~~] Who  
16 shall be served with the order and by what means.

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



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

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



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

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



1           (1) The interception shall be conducted in such a way as  
2           to minimize the resulting invasion of privacy  
3           including but not limited to the following methods of  
4           minimization:

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

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

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

17          (A) The parties to the conversation;

18          (B) The particular offense being investigated;

19          (C) The subject matter of the conversation;

20          (D) The subject matter of previous conversations

21          between the same parties and whether any

22          incriminating statements occurred; and



1 (E) The hour and day of conversation.

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

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



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



1           shall be a prerequisite for the use or disclosure  
2           of the contents of any wire, oral, or electronic  
3           communication or evidence derived therefrom under  
4           section 803-45(c).

5           (2) Applications made and orders granted under this part,  
6           ~~[transcripts of hearings on applications,]~~ and  
7           evidence obtained through court-ordered interceptions  
8           shall be sealed by the designated ~~[circuit court]~~  
9           judge. Custody of the above shall be ~~[whenever]~~  
10          wherever the ~~[court]~~ designated judge directs.  
11          Applications and orders shall be disclosed only upon a  
12          showing of good cause before a designated judge and  
13          shall not be destroyed, except upon order of the  
14          designated judge, and, in any event, shall be kept for  
15          ten years.

16          (3) Any violation of the provisions of this subsection may  
17          be punished as contempt ~~[of]~~ by the ~~[issuing or~~  
18          ~~denying court.]~~ designated judge.

19          (4) Within a reasonable time but no later than ninety days  
20          after either the filing of an application for an  
21          approval under subsection (d) that is denied or the  
22          termination of the period of an order or extensions





1           thereof, the [~~issuing court~~] designated judge shall  
2           cause an inventory to be served[~~7~~] on the persons  
3           named in the order, on all other known parties to  
4           intercepted communications, and to [~~such~~] any other  
5           persons as the court may determine is in the interest  
6           of justice[~~7-an~~]. The inventory [~~which~~] shall include  
7           notice of:

- 8           (A) The fact of the entry of the order;  
9           (B) The date of the entry and the period of  
10           authorized, or approved interception; and  
11           (C) The fact [~~whether~~] that during the applicable  
12           time period, wire, oral, or electronic  
13           communications were or were not intercepted[~~7-and~~  
14           (D) ~~The fact whether any incriminating statements~~  
15           ~~were intercepted.~~].

16           The designated [~~circuit court~~] judge, upon the filing  
17           of a motion, [~~shall~~] may make available to [~~such~~] the  
18           person or the person's counsel for inspection after  
19           the inventory has been served all portions of the  
20           intercepted communications [~~which~~] that contain  
21           conversations of that person, applications, orders,  
22           [~~transcripts of hearing,~~] and other evidence obtained



1 as a result of the use of interception orders. The  
2 [~~court~~] designated judge may order [~~such~~] the  
3 additional disclosure as the [~~court~~] designated judge  
4 determines to be in the interest of justice. On an ex  
5 parte showing of good cause [~~to a court~~], the  
6 designated judge may permit the serving of the  
7 inventory required by this subsection [~~may~~] to be  
8 postponed.

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

21 (i) (1) Any aggrieved person in any trial, hearing, or  
22 proceeding in or before any court, department,



1 officer, agency, regulatory body, or other authority  
2 of this State, or a political subdivision thereof, may  
3 move to suppress the content of any intercepted wire,  
4 oral, or electronic communication, or evidence derived  
5 therefrom, on the grounds that:

6 (A) The communication was unlawfully intercepted;

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

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

12 Such motion shall be made before the trial, hearing,  
13 or proceedings unless there was no opportunity to make  
14 such motion or the person was not aware of the grounds  
15 of the motion. If the motion is granted, the contents  
16 of the intercepted wire, oral, or electronic  
17 communication, or evidence derived therefrom, shall be  
18 treated as having been obtained in violation of this  
19 part. The court, or other official before whom the  
20 motion is made, upon the filing of [~~such~~] the motion  
21 by the aggrieved person, [~~shall~~] may make available to  
22 the aggrieved person or the aggrieved person's counsel



1 for inspection portions of the recording [~~which~~] that  
2 contain intercepted communications of the defendant or  
3 evidence derived therefrom, the applications, orders,  
4 transcript of [~~hearing~~] testimony, and such additional  
5 evidence as the court determines to be in the interest  
6 of justice.

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

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

20 (B) From an order denying an application for an order  
21 of authorization or approval, and such an appeal  
22 shall be in camera and in preference to all other



1 pending appeals in accordance with rules  
2 promulgated by the supreme court.

3 (j) The requirements of subsections (a) (2) (B) and (c) (4)  
4 relating to the specification of the facilities from which, or  
5 the place where, the communication is to be intercepted do not  
6 apply if:

7 (1) In the case of an application with respect to the  
8 interception of an oral communication:

9 (A) The application is by an investigative or law  
10 enforcement officer and is approved by the  
11 attorney general, a county prosecuting attorney,  
12 or one of their designees;

13 (B) The application contains a full and complete  
14 statement as to why the specification is not  
15 practical and identifies the person committing  
16 the offense and whose communications are to be  
17 intercepted; and

18 (C) The designated judge finds that the specification  
19 is not practical; or

20 (2) In the case of an application with respect to a wire  
21 or electronic communication:



1           (A) The application is by an investigative or law  
2           enforcement officer and is approved by the  
3           attorney general, a prosecuting attorney, or one  
4           of their designees;

5           (B) The application identifies the person believed to  
6           be committing the offense and whose  
7           communications are to be intercepted and the  
8           applicant makes a showing of a purpose on the  
9           part of that person to thwart interception by  
10          changing facilities; and

11          (C) The designated judge finds that the purpose has  
12          been adequately shown.

13   An interception of a communication under an order with respect  
14   to which the requirements of subsections (a) (2) (B) and (c) (4) do  
15   not apply by reason of subsection (j) shall not begin until the  
16   facilities from which, or the place where the communication is  
17   to be intercepted, is ascertained by the person implementing the  
18   interception order. A provider of wire or electronic  
19   communications service that has received an order as provided  
20   for in subsection (d) may move the court to modify or quash the  
21   order on the ground that its assistance with respect to the  
22   interception cannot be performed in a timely or reasonable



1 manner. The court, upon notice to the State, shall decide the  
2 motion expeditiously.

3       **§803-47 Reports concerning intercepted wire, oral, or**  
4 **electronic communications; reports concerning pen registers and**  
5 **trap and trace devices.** (a) In January of each year, the  
6 attorney general and county prosecuting attorneys of this State  
7 shall report to the administrative director of the courts of  
8 this State and to the administrative office of the United States  
9 Courts:

- 10       (1) The fact that an order or extension was applied for;
- 11       (2) The kind of order or extension applied for;
- 12       (3) The fact that the order or extension was granted as  
13             applied for, was modified, or was denied;
- 14       (4) The period of interceptions authorized by the order,  
15             and the number and duration of any extensions of the  
16             order;
- 17       (5) The offense specified in the order or application, or  
18             extension of an order;
- 19       (6) The identity of the investigative or law enforcement  
20             officer and agency requesting the application and the  
21             person authorizing the request for application;

- 1 (7) The nature of the facilities from which or the place  
2 where communications were to be intercepted;
- 3 (8) A general description of the interceptions made under  
4 such order or extension, including:
- 5 (A) [~~the~~] The approximate nature and frequency of  
6 incriminating communications intercepted[~~τ~~];
- 7 (B) [~~the~~] The approximate nature and frequency of  
8 other communications intercepted[~~τ~~];
- 9 (C) [~~the~~] The approximate number of persons whose  
10 communications were intercepted[~~τ~~]; and
- 11 (D) [~~the~~] The approximate nature, amount, and cost of  
12 the [~~manpower~~] personnel and other resources used  
13 in the interceptions;
- 14 (9) The number of arrests resulting from interceptions  
15 made under [~~such~~] an order or extension of the order,  
16 and the offenses for which the arrests were made;
- 17 (10) The number of trials resulting from [~~such~~] the  
18 interceptions;
- 19 (11) The number of motions to suppress made with respect to  
20 [~~such~~] the interceptions[~~τ~~] and the number granted or  
21 denied;





1 (12) The number of convictions resulting from [~~such~~] the  
2 interceptions and the offenses for which the  
3 convictions were obtained and a general assessment of  
4 the importance of the interceptions;

5 (13) The information required by paragraphs (2) through (6)  
6 of this subsection with respect to orders or  
7 extensions obtained in a preceding calendar year and  
8 not yet reported; and

9 (14) Other information required by the rules and  
10 regulations of the administrative office of the United  
11 States Courts.

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

21 (c) The attorney general, at least twenty days prior to  
22 the convening of each regular session, shall annually report to



1 the legislature on the number of pen register orders and orders  
2 for trap and trace devices applied for by law enforcement  
3 agencies of the State.

4 **[{]§803-47.5[{]} Disclosure of contents of communication**  
5 **while in electronic storage.**

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

11 (2) A person or entity providing remote computing  
12 [~~services~~] service to the public shall not knowingly  
13 divulge to any person or entity the contents of any  
14 communication [~~which~~] that is carried or maintained on  
15 that service:

16 (A) On behalf of, and is either received by means of  
17 computer processing of communications or by  
18 electronic transmission, from [~~or created by~~  
19 ~~means of computer processing of communications~~  
20 ~~received by means of electronic transmissions~~  
21 ~~from~~] a subscriber or customer of [~~such~~] the  
22 service; and



1 (B) Solely for the purpose of providing storage [~~and~~  
2 or computer processing services to [~~such~~] the  
3 subscriber or customer, if the provider is not  
4 authorized to access the contents of [~~any such~~]  
5 those communications for purposes of providing  
6 any services other than storage or computer  
7 processing.

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

- 10 (1) To an addressee[~~r~~] or intended recipient of the  
11 communication[~~r~~] or [~~the~~] an agent of the  
12 [~~addressee's~~] addressee or intended [~~recipient's~~  
13 agent, of such communication] recipient;
- 14 (2) As otherwise authorized by a court order or search  
15 warrant;
- 16 (3) With the lawful consent of the originator, addressee,  
17 or intended recipient of [~~such~~] the communication, or  
18 the subscriber in the case of a remote computing  
19 service;
- 20 (4) To a person employed or authorized or whose facilities  
21 are used to forward [~~such~~] the communication to its  
22 destination;



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

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

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

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

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

20 (b) A governmental entity may require a provider of remote  
21 computing services to disclose the contents of any electronic



1 communication to which this subsection is made applicable by  
2 subsection (c) of this section:

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

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

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

12 (1) On behalf of, and received by electronic transmission  
13 from (or created by computer processing of  
14 communications received by electronic transmission  
15 from), a subscriber or customer of [~~such~~] the remote  
16 computing service; and

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



- 1 (d) (1) A provider of electronic communication service or  
2 remote computing [~~services~~] service may disclose a  
3 record or other information pertaining to a subscriber  
4 to, or customer of [~~such~~], the service (other than the  
5 contents of any electronic communication) to any  
6 person other than a governmental entity.
- 7 (2) A provider of electronic communication service or  
8 remote computing [~~services~~] service shall disclose a  
9 record or other information pertaining to a subscriber  
10 to, or customer of [~~such~~], the service (other than the  
11 contents of an electronic communication) to a  
12 governmental entity only when:
- 13 (A) Presented with a search warrant;
- 14 (B) Presented with a court order for [~~such~~] the  
15 disclosure;
- 16 (C) The consent of the subscriber or customer to  
17 [~~such~~] the disclosure has been obtained; or
- 18 (D) Presented with an administrative subpoena [~~issued~~  
19 ~~pursuant to section 28-2.5~~] authorized by  
20 statute, an attorney general subpoena, or a grand  
21 jury or trial subpoena, which seeks the  
22 disclosure of information concerning electronic



1 communication, including but not limited to the  
2 name, address, local and long distance telephone  
3 [~~te~~] billing records, telephone number or other  
4 subscriber number or identity, and length of  
5 service of a subscriber to or customer of the  
6 service, and the types of [~~service utilized by~~]  
7 services the subscriber or customer utilized.

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

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



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

6 (g) A provider of wire or electronic communication  
7 services or a remote computing service, upon the request of a  
8 governmental entity, shall take all necessary steps to preserve  
9 records and other evidence in its possession pending the  
10 issuance of a court order or other process. Records shall be  
11 retained for a period of ninety days, which shall be extended  
12 for an additional ninety-day period upon a renewed request by  
13 the governmental entity.

14 ~~[+]~~§803-47.7~~[+]~~ **Backup preservation.** (a) A governmental  
15 entity may include in its court order a requirement that the  
16 service provider create a backup copy of the contents of the  
17 electronic communication without notifying the subscriber or  
18 customer. The service provider shall create ~~[such]~~ the backup  
19 copy as soon as practicable, consistent with its regular  
20 business practices, and shall confirm to the governmental entity  
21 that ~~[such a]~~ the backup copy has been made. ~~[Such]~~ The backup  
22 copy shall be created within two business days after receipt by





1 the service provider of [a] the subpoena or court order [~~by the~~  
2 ~~service provider~~].

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

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

9 (1) The delivery of the information; or

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

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

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

19 (2) Has not initiated proceedings to challenge the  
20 [~~governmental entity's~~] request of the governmental  
21 entity.



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

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

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

18 (f) Upon receiving a copy of the motion from the  
19 subscriber or customer, the governmental agency shall file a  
20 sworn response to the court to which the motion is assigned.  
21 The response shall be filed within fourteen days. The response  
22 may ask the court for an in camera review, but must state



1 reasons justifying such a review. If the court is unable to  
2 rule solely on the motion or application and response submitted,  
3 the court may conduct such additional proceedings as it deems  
4 appropriate. A ruling shall be made as soon as practicable  
5 after the filing of the governmental entity's response.

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

20 **[+]§803-47.8[+] Delay of notification.** (a) A  
21 governmental entity may as part of a request for a court order  
22 include a provision that notification be delayed for a period



1 not exceeding ninety days if the court determines that  
2 notification of the existence of the court order may have an  
3 adverse result.

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

- 6 (1) Endangering the life or physical safety of an  
7 individual;
- 8 (2) Flight from prosecution;
- 9 (3) Destruction of or tampering with evidence;
- 10 (4) Intimidation of a potential witness; or
- 11 (5) Otherwise seriously jeopardizing an investigation or  
12 unduly delaying a trial.

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

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

20 (1) States with reasonable specificity the nature of the  
21 law enforcement inquiry; and

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



- 1 (A) [~~That information~~] Information maintained for  
2 [~~such~~] the customer or subscriber by the service  
3 provider or request was supplied to or requested  
4 by that governmental authority and the date on  
5 which the supplying or request took place;
- 6 (B) [~~That notification~~] Notification of [~~such~~] the  
7 customer or subscriber was delayed;
- 8 (C) [~~What~~] The governmental entity or court that made  
9 the certification or determination upon which the  
10 delay was made; and
- 11 (D) [~~Which~~] The provision of this part that allowed  
12 [~~such~~] the delay.
- 13 (e) A governmental entity may apply to the [~~circuit court~~]  
14 designated judge [~~by the chief justice of the Hawaii supreme~~  
15 ~~court~~] or any other circuit judge or district court judge, if a  
16 circuit court judge has not yet been designated by the chief  
17 justice of the Hawaii supreme court, or is otherwise  
18 unavailable, for an order commanding a provider of an electronic  
19 communication service or remote computing service to whom a  
20 search warrant, or court order is directed, not to notify any  
21 other person of the existence of the search warrant, or court  
22 order for such period as the court deems appropriate not to



1 exceed ninety days. The court shall enter [~~such an~~] the order  
2 if it determines that there is reason to believe that  
3 notification of the existence of the search warrant, or court  
4 order will result in:

- 5 (1) Endangering the life or physical safety of an  
6 individual;
- 7 (2) Flight from prosecution;
- 8 (3) Destruction of or tampering with evidence;
- 9 (4) Intimidation of [~~a~~] potential [~~witness,~~] witnesses; or
- 10 (5) Otherwise seriously jeopardizing an investigation or  
11 unduly delaying a trial.

12 **[~~§~~803-47.9~~]~~ Cost reimbursement.** (a) A government  
13 entity obtaining the contents of communications, records, or  
14 other information shall [~~reimburse any~~] pay to the person or  
15 entity [~~reasonable fees for~~] providing or assembling [~~such~~] the  
16 information a fee for reimbursement or costs that are reasonably  
17 necessary and that have been directly incurred in searching for,  
18 assembling, reproducing, or otherwise providing the information.

19 [~~Such~~] The reimbursable costs shall include any costs due to  
20 necessary disruption of normal operations of any electronic  
21 communication service or remote computing service [~~which~~] that  
22 was occasioned by the governmental needs.



1       (b) The amount of the fee provided by subsection (a) shall  
2 be as mutually agreed by the governmental entity and the person  
3 or entity providing the information or, in the absence of  
4 agreement, shall be as determined by the designated court that  
5 issued the order for production of the information or the court  
6 before which a criminal prosecution relating to the information  
7 would be brought, if no court order was issued for production of  
8 the information.

9       (c) The requirement of subsection (a) does not apply with  
10 respect to records or other information maintained by a  
11 communication common carrier that relate to telephone toll  
12 records and telephone listings obtained under section 803-47.6.  
13 However, the court may order a payment as described in  
14 subsection (a), if the court determines the information required  
15 is unusually voluminous in nature or otherwise caused an undue  
16 burden on the provider.

17       **§803-48 Recovery of civil damages authorized.** Any person  
18 whose wire, oral, or electronic communication is accessed,  
19 intercepted, disclosed, or used in violation of this part shall  
20 (1) have a civil cause of action against any person who  
21 accesses, intercepts, discloses, or uses, or procures any other  
22 person to access, intercept, disclose, or use [~~such~~] the



1 communications, and (2) be entitled to recover from any such  
2 person:

3 (A) The greater of (i) the sum of the actual damages  
4 suffered by the plaintiff and any profits made by the  
5 violator as a result of the violation, or (ii)  
6 statutory damages of [~~whichever is~~] the greater of  
7 \$100 a day for each day of violation or \$10,000;

8 (B) Punitive damages, where appropriate; and

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

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

16 **§803-49 Severability.** If any portion or subsection of  
17 this part or the application thereof to any person or  
18 circumstances is invalid, such invalidity shall not affect other  
19 sections or applications of the part which can be given effect  
20 without the invalid section or application, and to this end the  
21 provisions of this part are declared to be severable."

22 SECTION 5. This Act does not affect rights and duties



1 that matured, penalties that were incurred, and proceedings that  
2 were begun, before its effective date.

3 SECTION 6. Statutory material to be repealed is bracketed  
4 and stricken. New statutory material is underscored.

5 SECTION 7. This Act shall take effect upon its approval.



SB965, SD2, HD1, CD1

**Report Title:**

Electronic Surveillance; Wiretapping

**Description:**

Amends State's electronic eavesdropping statute. (CD1)

