
A BILL FOR AN ACT

RELATING TO ELECTRONIC SURVEILLANCE.

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

1 SECTION 1. Chapter 803, Hawaii Revised Statutes, is
2 amended by adding a new part to be appropriately designated and
3 to read as follows:

4 **"PART . WIRETAPPING AND ELECTRONIC SURVEILLANCE**

5 A. GENERAL PROVISIONS

6 **§803-A Definitions.** As used in this part unless the
7 context clearly requires otherwise:

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

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

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

17 "Communication common carrier" means any person engaged as
18 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. If a circuit court judge has not been
13 designated by the chief justice or is unavailable, a "designated
14 judge" shall include any circuit court judge or district court
15 judge.

16 "Electronic communication" means any transfer of signs,
17 signals, writing, images, sounds, data, or intelligence of any
18 nature transmitted in whole or in part by a wire, radio,
19 electromagnetic, photoelectronic, or photo-optical system, but
20 does not include:

21 (1) Any wire or oral communication;



1 (2) Any communication made through a tone-only paging
2 device;

3 (3) Any communication from a tracking device; or

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

7 "Electronic communication service" means any service that
8 provides to users thereof the ability to send or receive wire or
9 electronic communications.

10 "Electronic communication system" means any wire, radio,
11 electromagnetic, photo-optical, or photoelectronic facilities
12 for the transmission of electronic communications and any
13 computer facilities or related electronic equipment for the
14 electronic storage of these communications.

15 "Electronic, mechanical, or other device" means any device
16 or apparatus that can be used to intercept a wire, oral, or
17 electronic communication other than:

18 (1) Any telephone or telegraph instrument, equipment, or
19 facility, or any component thereof:

20 (A) Furnished to the subscriber or user by a provider
21 of wire or electronic communication service in
22 the ordinary course of its business and being



1 used by the subscriber or user in the ordinary
2 course of its business or furnished by the
3 subscriber or user for connection to the
4 facilities of the service and used in the
5 ordinary course of its business; or

6 (B) Being used by a provider of wire or electronic
7 communication service in the ordinary course of
8 its business or by an investigative or law
9 enforcement officer in the ordinary course of the
10 officer's duties; and

11 (2) A hearing aid or similar device being used to correct
12 subnormal hearing to a level not better than average.

13 "Electronic storage" means:

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

17 (2) Any storage of the communication by an electronic
18 communication service for purposes of backup
19 protection of the communication.

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



1 "Investigative or law enforcement officer" means any
2 officer of the State, county, or United States, who is empowered
3 by law to conduct investigations or make arrests for offenses
4 enumerated in this part.

5 "Oral communication" means any utterance by a person
6 exhibiting an expectation that the utterance is not subject to
7 interception under circumstances justifying that expectation,
8 but the term does not include any electronic communication.

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

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



1 "Person" means any employee or agent of the United States,
2 any state, or any county; any individual; partnership;
3 association; joint stock company; trust; or corporation.

4 "Readily accessible to the general public" means, with
5 respect to a radio communication, that the communication is 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 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
15 tone-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 that permits the tracking of the movement of a person or object,
8 but does not include 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 the motor vehicle or other
13 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 that captures the
17 incoming electronic or other impulses that identify the
18 originating number of an instrument or device from which a wire
19 or electronic communication was transmitted.

20 "User" means any person or entity that:

21 (1) Uses an electronic communication service; and



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

3 "Wire communication" means any aural transfer made, in
4 whole or in part, through the use of facilities for the
5 transmission of communications by the aid of wire, cable, or
6 other similar connection between the point of origin and the
7 point of reception (including the use of such connection in a
8 switching station). The term "wire communication" also includes
9 any electronic storage of the communication.

10 B. WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS

11 **§803-B Prohibited interception or disclosure of wire,**

12 **oral, or electronic communications.** (a) A person, not entitled
13 to an exception within this section, commits the offense of
14 prohibited interception or disclosure of wire, oral, or
15 electronic communications if the person:

16 (1) Intentionally intercepts, attempts to intercept, or
17 solicits any other person to intercept or attempt to
18 intercept any wire, oral, or electronic communication;

19 (2) Intentionally uses, attempts to use, or solicits any
20 other person to use or attempt to use any electronic,
21 mechanical, or other device to intercept any oral
22 communication when:



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

4 (B) The device transmits communications by radio or
5 interferes with the transmission of the
6 communication;

7 (3) Intentionally discloses, or attempts to disclose, to
8 any other person the contents of any wire, oral, or
9 electronic communication, knowing or having reason to
10 know that the information was obtained through the
11 interception of a wire, oral, or electronic
12 communication in violation of this part;

13 (4) Intentionally uses, or attempts to use, the contents
14 of any wire, oral, or electronic communication,
15 knowing or having reason to know that the information
16 was obtained through the interception of a wire, oral,
17 or electronic communication in violation of this part;
18 or

19 (5) Intentionally discloses, or attempts to disclose, to
20 any other person the contents of any wire, oral, or
21 electronic communication, intercepted by means



1 authorized by subsection (b) (1), (2), or (3), or
2 section 803-H or 803-J; and

3 (A) Either:

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

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

11 (B) With the intent to improperly obstruct, impede,
12 or interfere with a duly authorized criminal
13 investigation.

14 (b) It shall not be unlawful under this part:

15 (1) For an operator of a switchboard or an officer,
16 employee, or agent of a provider of wire or electronic
17 communication service, whose facilities are used in
18 the transmission of a wire or electronic
19 communication, to intercept, disclose, or use that
20 communication in the normal course of employment while
21 engaged in any activity that is either a necessary
22 incident to the rendition of the operator's,



1 officer's, employee's, or agent's service, or for the
2 protection of the rights or property of the provider
3 of that service; provided that a provider of wire
4 communication service to the public shall not utilize
5 service observing or random monitoring, except for
6 mechanical or service quality control checks;

7 (2) Notwithstanding any other law to the contrary, for
8 providers of wire or electronic communication service
9 and their officers, employees, and agents, landlords,
10 custodians, or other persons authorized to provide
11 information, facilities, or technical assistance to
12 persons authorized by law to intercept wire, oral, or
13 electronic communications or to conduct electronic
14 surveillance, if the provider or its officers,
15 employees, or agents, landlord, custodian, or other
16 specified person has been provided with a court order
17 directing such assistance, signed by the designated
18 judge. No provider of wire or electronic
19 communication service, officer, employee, or agent
20 thereof, or landlord, custodian, or other specified
21 person shall disclose the existence of any
22 interception or surveillance or the device used to



1 accomplish the interception or surveillance with
2 respect to which the person has been furnished an
3 order under this subpart, except as may otherwise be
4 required by the legal process and then only after
5 prior notification to the party that provided the
6 court order. Any such disclosure shall render the
7 person liable for the civil damages provided for in
8 section 803-L. No cause of action shall lie against
9 any provider of wire or electronic communication
10 service or its officers, employees, or agents,
11 landlord, custodian, or other specified person for
12 providing information, facilities, or assistance in
13 accordance with the terms of a court order under this
14 part;

- 15 (3) For an officer, employee, or agent of the Federal
16 Communications Commission, in the normal course of the
17 officer's, employee's, or agent's employment and in
18 discharge of the monitoring responsibilities exercised
19 by the Commission in the enforcement of title 47,
20 chapter 5, of the United States Code, to intercept a
21 wire or electronic communication or oral communication



1 transmitted by radio or to disclose or use the
2 information thereby obtained;

3 (4) For a person acting under the color of law to
4 intercept a wire, oral, or electronic communication
5 when the person is a party to the communication or if
6 one of the parties to the communication has given
7 prior consent to the interception;

8 (5) For a person not acting under the color of law to
9 intercept a wire, oral, or electronic communication
10 when the person is a party to the communication or
11 when one of the parties to the communication has given
12 prior consent to the interception, unless the
13 communication is intercepted for the purpose of
14 committing any criminal or tortious act in violation
15 of the Constitution or laws of the United States or of
16 the State;

17 (6) For any person to intercept or access an electronic
18 communication made through an electronic communication
19 system that is configured so that the electronic
20 communication is readily accessible to the general
21 public;



1 (7) For any person to intercept any radio communication
2 that is transmitted:

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

6 (B) By any governmental, law enforcement, civil
7 defense, private land mobile, or public safety
8 communications system, including police and fire
9 that is readily accessible to the general public;

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

14 (D) By any marine or aeronautical communications
15 system;

16 (8) For any person to engage in any conduct that:

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

19 (B) Is excepted from the application of section
20 705(a) of the Communications Act of 1934 by
21 section 705(b) of that Act (47 U.S.C. §605);



- 1 (9) For any person to intercept any wire or electronic
2 communication, the transmission of which is causing
3 harmful interference to any lawfully operating station
4 or consumer electronic equipment, to the extent
5 necessary to identify the source of the interference;
- 6 (10) For other users of the same frequency to intercept any
7 radio communication made through a system that
8 utilizes frequencies monitored by individuals engaged
9 in the provision or the use of the system, if the
10 communication is not scrambled or encrypted;
- 11 (11) For a person to use a pen register or a trap and trace
12 device as those terms are defined in this part; or
- 13 (12) For a provider of electronic communication service to
14 record the fact that a wire or electronic
15 communication was initiated or completed in order to
16 protect the provider, another provider furnishing
17 service toward the completion of the wire or
18 electronic communication, or a user of that service
19 from the fraudulent, unlawful, or abusive use of the
20 service.
- 21 (c) Except as provided in this section, a person or entity
22 providing an electronic communication service to the public



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

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

- 10 (1) As otherwise authorized in subsection (b)(1) or (2) or
11 section 803-I;
- 12 (2) With the lawful consent of the originator, addressee,
13 or intended recipient of the communication;
- 14 (3) To a person employed or authorized, or whose
15 facilities are used, to forward the communication to
16 its destination; or
- 17 (4) That was inadvertently obtained by the service
18 provider and that appears to pertain to the commission
19 of a crime, if the divulgence is made to a law
20 enforcement agency.
- 21 (d) Prohibited interception or disclosure of wire, oral,
22 or electronic communications is a class C felony.



1 **§803-C Defenses.** (a) In a prosecution for prohibited
2 interception or disclosure of wire, oral, or electronic
3 communications, it is a defense that reduces the penalty to a
4 misdemeanor if:

5 (1) The offense is a first offense;

6 (2) The interception or disclosure was not for a tortious
7 or illegal purpose or for purposes of direct or
8 indirect commercial advantage or private commercial
9 gain; and

10 (3) The wire or electronic communication intercepted or
11 disclosed is a radio communication that is not
12 scrambled, encrypted, or transmitted using modulation
13 techniques, the essential parameters of which have
14 been withheld from the public with the intention of
15 preserving the privacy of such communication.

16 (b) In a prosecution for prohibited interception or
17 disclosure of wire, oral, or electronic communications, it is a
18 defense that the conduct with which the defendant is charged
19 with consists of or relates to the interception of a satellite
20 transmission that is not encrypted or scrambled and that is
21 transmitted:



- 1 (1) To a broadcasting station for purposes of
- 2 retransmission to the general public; or
- 3 (2) As an audio subcarrier intended for redistribution to
- 4 facilities open to the public, but not including data
- 5 transmissions or telephone calls.

6 **§803-D Civil actions.** (a) A person who engages in the
7 following conduct shall be subject to suit by the State, if the
8 intercepted communication is:

- 9 (1) A private satellite video communication that is not
- 10 scrambled or encrypted and the conduct in violation of
- 11 this part is the private viewing of that communication
- 12 and not for a tortious or illegal purpose or for
- 13 purposes of direct or indirect commercial advantage or
- 14 private commercial gain; or
- 15 (2) A radio communication that is transmitted on
- 16 frequencies allocated under subpart D of part 74 of
- 17 the rules of the Federal Communications Commission
- 18 that is not scrambled or encrypted and the conduct in
- 19 violation of this part is for tortious or illegal
- 20 purpose or for purposes of direct or indirect
- 21 commercial advantage or private commercial gain.

22 (b) In an action under this section:



1 (1) If the violation under this subpart is a first offense
2 for the person under subsection (a)(1) and the person
3 has not been found liable in a civil action under
4 section 803-L, the State shall be entitled to
5 appropriate injunctive relief; or

6 (2) If the violation of this subpart is a second or
7 subsequent offense under subsection (a)(1) or the
8 person has been found liable in any prior civil action
9 under section 803-L, the person shall be subject to a
10 mandatory \$500 civil fine.

11 (c) The court may use any means within its authority to
12 enforce an injunction issued under this section and shall impose
13 a civil fine of not less than \$500 for each violation of the
14 injunction.

15 **§803-E Prohibited manufacture, distribution, possession,**
16 **or advertising of wire, oral, or electronic communication**
17 **intercepting device.** (a) A person shall not be entitled to an
18 exception under this section, if the person commits the offense
19 of prohibited manufacture, distribution, possession, or
20 advertising of a wire, oral, or electronic communication
21 intercepting device if the person intentionally:



1 (1) Sends through the mail or sends or carries in
2 intrastate, interstate, or foreign commerce any
3 electronic, mechanical, or other device, knowing or
4 having reason to know that the design of the device
5 renders it primarily useful for the purpose of the
6 surreptitious interception of wire, oral, or
7 electronic communications;

8 (2) Manufactures, assembles, possesses, or sells any
9 electronic, mechanical, or other device, knowing or
10 having reason to know that the design of the device
11 renders it primarily useful for the purpose of the
12 surreptitious interception of wire, oral, or
13 electronic communications and that the device or any
14 component thereof has been or will be sent through the
15 mail or transported in intrastate, interstate, or
16 foreign commerce; or

17 (3) Places in any newspaper, magazine, handbill, or other
18 publication, knowing or having reason to know that the
19 advertisement will be sent through the mail or
20 transported in intrastate, interstate, or foreign
21 commerce, any advertisement of:



1 (A) Any electronic, mechanical, or other device,
2 knowing or having reason to know that the design
3 of the device renders it primarily useful for the
4 purpose of the surreptitious interception of
5 wire, oral, or electronic communications; or
6 (B) Any other electronic, mechanical, or other
7 device, where the advertisement promotes the use
8 of the device for the purpose of the
9 surreptitious interception of wire, oral, or
10 electronic communications.

11 (b) It shall not be unlawful under this section for:
12 (1) A provider of wire or electronic communication service
13 or an officer, agent, or employee of, or a person
14 under contract with such a provider in the normal
15 course of the business of providing that wire or
16 electronic communication service;
17 (2) An officer, agent, or employee of, or a person under
18 contract with, the State or a county, in the normal
19 course of the activities of the State or a county; or
20 (3) A person acting under the color of law;
21 to send through the mail, send or carry in intrastate,
22 interstate, or foreign commerce, or manufacture, assemble,

1 possess, or sell any electronic, mechanical, or other device,
2 knowing or having reason to know that the design of the device
3 renders it primarily useful for the purpose of surreptitious
4 interception of wire, oral, or electronic communications.

5 (c) Prohibited manufacture, distribution, possession, or
6 advertising of wire, oral, or electronic communication
7 intercepting device is a class C felony.

8 **§803-F Forfeiture of wire, oral, or electronic**
9 **communication intercepting devices.** Any electronic, mechanical,
10 or other device used, sent, carried, manufactured, assembled,
11 possessed, sold, or advertised, or otherwise distributed in
12 violation of this part shall be subject to seizure and
13 forfeiture under chapter 712A.

14 **§803-G Prohibition of use as evidence of intercepted wire**
15 **or oral communications.** No part of the contents of any wire or
16 oral communication and no evidence derived therefrom may be
17 received into evidence at any trial, hearing, or other
18 proceeding in or before any court, grand jury, department,
19 officer, agency, regulatory body, legislative committee, or
20 other authority of the State or a county, if the disclosure of
21 that information would be in violation of this part.



1 **§803-H Authorization for interception of wire, oral, or**
2 **electronic communications.** The attorney general or designee, or
3 the prosecuting attorney of each county or a designee may
4 authorize an application to a designated judge for, and the
5 designated judge may grant, in conformity with section 803-J, an
6 order authorizing or approving the interception of wire, oral,
7 or electronic communications, by an investigative or law
8 enforcement officer or agency having responsibility for the
9 investigation of the offense that the application is made for,
10 if the interception might provide or has provided evidence of:

- 11 (1) Murder;
- 12 (2) Kidnapping;
- 13 (3) Felony criminal property damage involving the danger
14 of substantial bodily injury as defined in section
15 707-700;
- 16 (4) Organized crime;
- 17 (5) Extortion;
- 18 (6) Bribery of a juror, a witness, or a police officer;
- 19 (7) Receiving stolen property;
- 20 (8) Gambling;
- 21 (9) Distribution of dangerous, harmful, or detrimental
22 drugs;



- 1 (10) Money laundering;
- 2 (11) Racketeering activity as defined in section 842-1;
- 3 (12) A criminal offense against a victim who is a minor or
- 4 a sexually violent offense as those terms are defined
- 5 in section 846E-1;
- 6 (13) Violations relating to firearms or explosives;
- 7 (14) Any felony violation of this part;
- 8 (15) Any conspiracy to commit any offense described in this
- 9 section; or
- 10 (16) The location of any fugitive from justice charged with
- 11 an offense described in this section.

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



1 (b) Any investigative or law enforcement officer who, by
2 any means authorized by this part, has obtained knowledge of the
3 contents of any wire, oral, or electronic communication or
4 evidence derived therefrom may use the contents to the extent
5 the use is appropriate to the proper performance of the
6 officer's official duties.

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

14 (d) No otherwise privileged wire, oral, or electronic
15 communication intercepted in accordance with, or in violation
16 of, this part shall lose its privileged character.

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



1 and any evidence derived therefrom may be used under subsection
2 (c) when authorized or approved by a designated judge, if the
3 designated judge finds on a subsequent application that the
4 contents were otherwise intercepted in accordance with this
5 part. The subsequent application shall be made as soon as
6 practicable.

7 **§803-J Procedure for interception of wire, oral, or**
8 **electronic communications; application; order; remedies. (a)**

9 Each application for an order authorizing or approving the
10 interception of a wire, oral, or electronic communication under
11 this part shall be made in writing upon oath or affirmation to a
12 designated judge. The application shall state the applicant's
13 authority to make the application. Each application shall
14 include the following information:

15 (1) The identity of the investigative or law enforcement
16 officer making the application and the officer
17 authorizing the application;

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



- 1 (A) Details relating to the particular offense that
- 2 has been, is being, or is about to be committed;
- 3 (B) Except as provided in subsection (i), a
- 4 particular description of the nature and location
- 5 of the facilities from which or the place where
- 6 the communication is to be intercepted;
- 7 (C) A particular description of the type of
- 8 communications sought to be intercepted; and
- 9 (D) The identity of the person, if known, committing
- 10 the offense and whose communications are to be
- 11 intercepted;
- 12 (3) A full and complete statement as to whether other
- 13 investigative procedures have been tried and failed or
- 14 why they reasonably appear to be either unlikely to
- 15 succeed if tried or too dangerous;
- 16 (4) A statement of the period of time for which the
- 17 interception is required to be maintained; or if the
- 18 nature of the investigation is such that the
- 19 authorization for interception should not
- 20 automatically terminate when the described type of
- 21 communication has been first obtained, a particular
- 22 description of facts establishing probable cause to

1 believe that additional communications of the same
2 type will occur thereafter;

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

12 (6) When the application is for the extension of an order,
13 a statement setting forth the results thus far
14 obtained from the interception or a reasonable
15 explanation as to the failure to obtain any results.

16 (b) The designated judge may require the applicant to
17 furnish additional testimony or documentary evidence in support
18 of the application.

19 (c) Upon an application, the designated judge may enter an
20 ex parte order, as requested or as modified, authorizing or
21 approving interception of wire, oral, or electronic

1 communications, if the designated judge determines on the basis
2 of the facts submitted by the applicant that:

3 (1) There is probable cause to believe that a person is
4 committing, has committed, or is about to commit a
5 particular offense enumerated in section 803-H;

6 (2) There is probable cause to believe that particular
7 communications concerning that offense will be
8 obtained through the interception;

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

12 (4) Except as provided in subsection (i), there is
13 probable cause to believe that the facilities from
14 which or the place where the wire, oral, or electronic
15 communications are to be intercepted are being used or
16 are about to be used in connection with the commission
17 of such offense, or are leased to, listed in the name
18 of, or commonly used by that person.

19 (d) Each order authorizing or approving the interception
20 of any wire, oral, or electronic communication under this part
21 shall specify:

- 1 (1) The identify of the person, if known, whose
2 communications are to be intercepted;
- 3 (2) The nature and location of the communications
4 facilities or the place where the authority to
5 intercept is granted;
- 6 (3) A particular description of the type of communication
7 sought to be intercepted and a statement of the
8 particular offense to which it relates;
- 9 (4) The identity of the agency authorized to intercept the
10 communications and of the person authorizing the
11 application; and
- 12 (5) The period of time during which the interception is
13 authorized, including a statement as to whether the
14 interception is to terminate automatically upon the
15 described communication first being obtained.

16 Upon request of the applicant, an order authorizing the
17 interception of a wire, oral, or electronic communication under
18 this part shall direct that a provider of a wire or electronic
19 communication service, landlord, custodian, or other person
20 shall furnish the applicant as soon as practicable all
21 information, facilities, and technical assistance necessary to
22 accomplish the interception unobtrusively and with a minimum of



1 interference with the services that the service provider,
2 landlord, custodian, or other person whose communications are to
3 be intercepted. Any provider of wire or electronic
4 communication service, landlord, custodian, or other person
5 furnishing the facilities or technical assistance shall be
6 compensated by the applicant for reasonable expenses incurred in
7 providing the facilities or assistance.

8 (e) No order entered under this section shall authorize or
9 approve the interception of any wire, oral, or electronic
10 communication for any period longer than is necessary to achieve
11 the objective of the authorization, and in no event for longer
12 than thirty days. The thirty-day period begins on the day the
13 investigative or law enforcement officer first begins to conduct
14 an interception under the order or ten days after the order is
15 entered. Extensions of an order may be granted, but only upon
16 an application for an extension made in accordance with
17 subsection (a) and the court making the findings required by
18 subsection (c). The period of extension shall be no longer than
19 the designated judge deems necessary to achieve the purposes for
20 which it was granted and in no event for longer than thirty
21 days. Every order and extension thereof shall contain a
22 provision that the authorization to intercept shall be executed



1 as soon as practicable, shall be conducted in such a way so as
2 to minimize the interception of communications not otherwise
3 subject to interception under this part, and shall terminate
4 upon attainment of the authorized objective, or in any event in
5 thirty days. If the intercepted communication is in a code or
6 foreign language, and an expert in that foreign language or code
7 is not reasonably available during the interception period,
8 interpretation may be accomplished as soon as practicable after
9 the interception.

10 An interception under this part may be conducted, in whole
11 or in part, by investigative or law enforcement officers or by
12 an individual operating under a contract with the State or a
13 county, acting under the supervision of an investigative or law
14 enforcement officer authorized to conduct the interception.

15 (f) Whenever an order authorizing interception is entered
16 pursuant to this part, the order may require reports to be made
17 to the designated judge who issued the order showing what
18 progress has been made toward achievement of the authorized
19 objective and the need for continued interception. The reports
20 shall be made at such intervals as the designated judge may
21 require.



1 (g) The requirements for the contents of communication,
2 applications, violations, and reasonable time shall be in
3 accordance with this subsection:

4 (1) The contents of any wire, oral, or electronic
5 communication intercepted by any means authorized by
6 this part shall be recorded on tape or wire or other
7 comparable device, if technically possible. The
8 recording of the contents of any wire, oral, or
9 electronic communication under this subsection shall
10 be done to protect the recording from being edited or
11 otherwise altered. Immediately upon the expiration of
12 the time period provided in the order, or extensions
13 thereof, the recording shall be made available to the
14 designated judge issuing the order and sealed under
15 the designated judge's directions. Custody of the
16 recording shall be determined by order of the
17 designated judge. Recordings shall not be destroyed,
18 except upon an order of the designated judge, and, in
19 any event, shall be kept for ten years. Duplicate
20 recordings may be made for use or disclosure pursuant
21 to section 803-I(a) and (b) for investigations. The
22 presence of the seal required by this subsection, or a



1 satisfactory explanation for the absence thereof,
2 shall be a prerequisite for the use or disclosure of
3 the contents of any wire, oral, or electronic
4 communication or evidence derived therefrom under
5 section 803-I(c);

6 (2) Applications made and orders granted under this part
7 shall be sealed by the designated judge. Custody of
8 the applications and orders shall be wherever the
9 designated judge directs. Applications and orders
10 shall be disclosed only upon a showing of good cause
11 before a designated judge and shall not be destroyed,
12 except upon order of the designated judge, and, in any
13 event, shall be kept for ten years;

14 (3) Any violation of this subsection may be punished as
15 contempt by the designated judge;

16 (4) Within a reasonable time, but not later than ninety
17 days after either the filing of an application for an
18 order of approval under subsection (d) that is denied
19 or the termination of the period of an order or
20 extensions thereof, the designated judge shall cause
21 to be served an inventory on the persons named in the
22 order or application, and any other parties to



1 intercepted communications that the designated judge
2 determines may receive service in the interest of
3 justice. The inventory shall include notice of:

4 (A) The fact of the entry of the order or the
5 application;

6 (B) The date of the entry, and the period of time
7 authorized, approved, or disapproved, or the
8 denial of the application; and

9 (C) The fact that during the applicable time period,
10 wire, oral, or electronic communications were or
11 were not intercepted; and

12 (5) The designated judge, upon the filing of a motion and
13 in the designated judge's discretion, may make
14 available to the person or the person's counsel for
15 inspection those portions of the intercepted
16 communications, applications, and orders as the
17 designated judge determines to be in the interest of
18 justice. On an ex parte showing of good cause, the
19 designated judge may permit the serving of the
20 inventory required by this subsection to be postponed.

21 (h) As provided in section 641-13, the State shall have
22 the right to appeal from an order granting a motion to suppress



1 or the denial of an application for an order of approval, if the
2 attorney general or the prosecuting attorney of a county or
3 their designees certify to the designated judge or other
4 official granting the motion or denying the application that the
5 appeal is not taken for purposes of delay. The appeal shall be
6 taken within thirty days after the date the order was entered
7 and shall be diligently prosecuted. If the appeal is from an
8 order denying an application for an order of authorization or
9 approval, the appeal shall be in camera and have priority over
10 all other pending appeals in accordance with rules adopted by
11 the supreme court.

12 (i) The requirements of subsections (a)(2)(B) and (c)(4)
13 relating to the specification of the facilities from which, or
14 the place where, the communication is to be intercepted do not
15 apply if:

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

18 (A) The application is by an investigative or law
19 enforcement officer and is approved by the
20 attorney general, a county prosecuting attorney,
21 or one of their designees;



- 1 (B) The application contains a full and complete
2 statement as to why the specification is not
3 practical and identifies the person committing
4 the offense and whose communications are to be
5 intercepted; and
- 6 (C) The designated judge finds that the specification
7 is not practical; or
- 8 (2) In the case of an application with respect to a wire
9 or electronic communication:
- 10 (A) The application is by an investigative or law
11 enforcement officer and is approved by the
12 attorney general, a prosecuting attorney, or one
13 of their designees;
- 14 (B) The application identifies the person believed to
15 be committing the offense and whose
16 communications are to be intercepted and the
17 applicant makes a showing of a purpose on the
18 part of that person to thwart interception by
19 changing facilities; and
- 20 (C) The designated judge finds that the purpose has
21 been adequately shown.



1 An interception of a communication under an order with respect
2 to which the requirements of subsections (a)(2)(B) and (c)(4) do
3 not apply by reason of subsection (i) shall not begin until the
4 facilities from which, or the place where the communication is
5 to be intercepted, is ascertained by the person implementing the
6 interception order. A provider of wire or electronic
7 communications service that has received an order as provided
8 for in subsection (d) may move the court to modify or quash the
9 order on the ground that its assistance with respect to the
10 interception cannot be performed in a timely or reasonable
11 manner. The court, upon notice to the State, shall decide the
12 motion expeditiously.

13 **§803-K Reports concerning intercepted wire, oral, or**
14 **electronic communications.** (a) Within thirty days after either
15 the expiration of an order or each extension thereof entered
16 under section 803-J, or the denial of an order approving an
17 interception, the designated judge shall report to the
18 administrative director of the courts:

- 19 (1) The fact that an order or extension was applied for;
20 (2) The kind of order or extension applied for, including
21 whether the order was an order with respect to which
22 the requirements of section 803-J(a)(2)(B) and



1 803-J(c)(4) did not apply by reason of section

2 803-J(i);

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

5 (4) The period of interceptions authorized by the order
6 and the number and duration of any extensions of the
7 order;

8 (5) The offense specified in the order or application, or
9 extension of the order;

10 (6) The identity of the applying investigative or law
11 enforcement officer and agency making the application
12 and the person authorizing the application; and

13 (7) The nature of the facilities from which or the place
14 where communications were to be intercepted.

15 (b) By January 1 of each year, the attorney general and
16 the county prosecutors shall report to the administrative
17 director of the courts:

18 (1) Information required by subsection (a) with respect to
19 each application for an order or extension made during
20 the preceding calendar year;

21 (2) A general description of the interceptions made under
22 the order or extension, including:



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

1 (8) Other information required by the office of the
2 administrative director of the courts.

3 (c) In March of each year, the administrative director of
4 the courts shall transmit to the legislature a full and complete
5 report concerning the number of applications for orders
6 authorizing or approving the interception of wire, oral, or
7 electronic communications pursuant to this part and the number
8 of orders and extensions granted or denied pursuant to this part
9 during the preceding calendar year. The report shall include a
10 summary and analysis of the data required to be filed with the
11 administrative director of the courts in subsections (a) and
12 (b). The administrative director of the courts may issue
13 binding guidelines dealing with the content and form of the
14 reports required to be filed by subsections (a) and (b).

15 **§803-L Recovery of civil damages authorized.** (a) Except
16 as provided in section 803-B(b), any person whose wire, oral, or
17 electronic communication is intercepted, disclosed, or
18 intentionally used in violation of this subpart may recover in a
19 civil action such relief as may be appropriate from the person
20 or entity that engaged in the violation.

21 (b) In an action under this section, appropriate relief
22 includes:

1 (1) Preliminary and other equitable or declaratory relief
2 as may be appropriate;

3 (2) Damages under subsection (c) and punitive damages in
4 appropriate cases; and

5 (3) A reasonable attorney's fee and other litigation costs
6 reasonably incurred.

7 (c) In an action under this section, if the conduct in
8 violation of this subpart is the private viewing of a private
9 satellite video communication that is not scrambled or encrypted
10 or if the communication is a radio communication that is
11 transmitted on frequencies allocated under subpart D of part 74
12 of the rules of the Federal Communications Commission that is
13 not scrambled or encrypted and the conduct is not for a tortious
14 or illegal purpose or for purposes of direct or indirect
15 commercial advantage or private commercial gain, the court shall
16 assess the damages as follows:

17 (1) If the person who engaged in that conduct has not
18 previously been enjoined under section 803-D and has
19 not been found liable in a prior civil action under
20 this section, the court shall assess the greater of
21 the sum of actual damages suffered by the plaintiff or



1 statutory damages of not less than \$50 and not more
2 than \$500; or

3 (2) If, on at least one prior occasion, the person who
4 engaged in that conduct has been enjoined under
5 section 803-D or has been found liable in a civil
6 action under this section, the court shall assess the
7 greater of the sum of actual damages suffered by the
8 plaintiff or statutory damages of not less than \$100
9 and not more than \$1,000.

10 (d) In any other action under this section, the court may
11 assess as damages the greater of:

12 (1) The sum of the actual damages suffered by the
13 plaintiff and any profits made by the violator as a
14 result of the violation; or

15 (2) Statutory damages of the greater of \$100 a day for
16 each day of violation or \$10,000.

17 (e) A civil action under this section shall not be
18 commenced later than two years after the date upon which the
19 claimant first has a reasonable opportunity to discover the
20 violation.

21 **§803-M Injunction against illegal interception.** Whenever
22 it appears that any person is engaged or is about to engage in



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

15 C. STORED COMMUNICATIONS

16 **§803-N Unlawful access to stored communications.** (a) A
17 person commits the offense of unlawful access to stored
18 communications if, without authorization as provided in
19 subsection (d), the person:

- 20 (1) Intentionally accesses without authorization a
21 facility through which an electronic communication
22 service is provided; or



1 (2) Intentionally exceeds an authorization to access that
2 facility; and
3 thereby obtains, alters, or prevents authorized access to a wire
4 or electronic communication while it is in electronic storage in
5 the system.

6 (b) Unlawful access to stored communications is a
7 misdemeanor, except as provided by subsection (c).

8 (c) Unlawful access to stored communications is a class C
9 felony if:

10 (1) Committed for purposes of commercial advantage,
11 malicious destruction or damage, or private commercial
12 gain; and

13 (2) The person committing the unlawful access to stored
14 communications has been previously convicted of
15 unlawful access to stored communications.

16 (d) Subsections (a), (b), and (c) shall not apply with
17 respect to conduct authorized:

18 (1) By the person or entity providing a wire or electronic
19 communications service;

20 (2) By a user of that service with respect to a
21 communication of or intended for that user; or

22 (3) In sections 803-J, 803-P, or 803-Q.



1 **§803-0 Disclosure of contents.** (a) Except as provided in
2 subsection (b):

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

8 (2) A person or entity providing remote computing service
9 to the public shall not knowingly divulge to any
10 person or entity the contents of any communication
11 that is carried or maintained on that service:

12 (A) On behalf of, and is either received or created
13 by means of computer processing of communications
14 or by electronic transmission, from a subscriber
15 or customer of the service; and

16 (B) Solely for the purpose of providing storage or
17 computer processing services to the subscriber or
18 customer, if the provider is not authorized to
19 access the contents of those communications for
20 purposes of providing any services other than
21 storage or computer processing.



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

3 (1) To an addressee or intended recipient of the
4 communication or an agent of the addressee or intended
5 recipient;

6 (2) As otherwise authorized in section 803-B(b), 803-I, or
7 803-P;

8 (3) With the lawful consent of the originator or an
9 addressee or intended recipient of the communication,
10 or the subscriber in the case of remote computer
11 service;

12 (4) To a person employed or authorized or whose facilities
13 are used to forward the communication to its
14 destination;

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

18 (6) To a law enforcement agency if the contents:

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

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

1 **§803-P Requirements for governmental access.** (a) A
2 governmental entity may require the disclosure by a provider of
3 electronic communication service of the contents of an
4 electronic communication that is in electronic storage in an
5 electronic communications system for one hundred and eighty days
6 or less, pursuant to a warrant only. A governmental entity may
7 require the disclosure by a provider of electronic
8 communications services of the contents of an electronic
9 communication that has been in electronic storage in an
10 electronic communications system for more than one hundred and
11 eighty days by the means available under subsection (b).

12 (b) A governmental entity may require a provider of remote
13 computing service to disclose the contents of any electronic
14 communication to which this subsection is made applicable by
15 subsection (c) except that delayed notice may be given pursuant
16 to section 803-R:

- 17 (1) Without required notice to the subscriber or customer,
18 if the governmental entity obtains a warrant; or
19 (2) With prior notice from the governmental entity to the
20 subscriber or customer, if the governmental entity:

1 (A) Uses an administrative subpoena authorized by
2 statute or an attorney general subpoena or a
3 grand jury subpoena or a trial subpoena; or

4 (B) Obtains a court order for the disclosure under
5 subsection (h).

6 (c) Subsection (b) applies with respect to any electronic
7 communication that is held or maintained:

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

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

19 (d) Except as provided in subsection (c), a provider of
20 electronic communication service or remote computing service may
21 disclose a record or other information pertaining to a
22 subscriber to, or customer of, the service (not including the



1 contents of communications covered by this section) to any
2 person other than a governmental entity.

3 (e) A provider of electronic communication service or
4 remote computing service shall disclose a record or other
5 information pertaining to a subscriber to or customer of the
6 service (not including the contents of communications covered by
7 subsection (a) or (b) to a governmental entity only when the
8 governmental entity:

9 (1) Obtains a warrant;

10 (2) Obtains a court order for the disclosure under
11 subsection (h); or

12 (3) Has the consent of the subscriber or customer to the
13 disclosure.

14 (f) A provider of electronic communication service or
15 remote computing service shall disclose to a governmental entity
16 the name, address, local and long distance telephone billing
17 records, telephone number or other subscriber number or
18 identity, and length of service of a subscriber or customer of
19 the service and the types of services the subscriber or customer
20 utilized, when the governmental entity uses an administrative
21 subpoena authorized by statute, an attorney general subpoena, or



1 a grand jury subpoena or a trial subpoena or any means available
2 under subsection (e).

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

6 (h) A court order for disclosure under subsection (b) or
7 (e) may be issued by a district court judge or a designated
8 judge and shall issue only if the governmental entity offers
9 specific and articulable facts showing that there are reasonable
10 grounds to believe that the contents of a wire or electronic
11 communication, or the records or other information sought, are
12 relevant and material to an ongoing criminal investigation. A
13 court issuing an order pursuant to this section, on a motion
14 made promptly by the service provider, may quash or modify the
15 order if the information or records requested are unusually
16 voluminous in nature or compliance with the order otherwise
17 would cause an undue burden on the provider.

18 (i) 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



1 with the terms of a court order, warrant, subpoena, or
2 certification under this subpart.

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

11 **§803-Q Backup preservation.** (a) A governmental entity
12 acting under section 803-P(b) may include in its subpoena or
13 court order a requirement that the service provider to whom the
14 request is directed create a backup copy of the contents of the
15 electronic communications sought in order to preserve those
16 communications. Without notifying the subscriber or customer of
17 the subpoena or court order, the service provider shall create
18 the backup copy as soon as practicable, consistent with its
19 regular business practices, and shall confirm to the
20 governmental entity that the backup copy has been made. The
21 backup copy shall be created within two business days after
22 receipt by the service provider of the subpoena or court order.



1 (b) Notice to the subscriber or customer shall be made by
2 the governmental entity within three days after receipt of the
3 confirmation that a backup has been made, unless notice is
4 delayed pursuant to section 803-R(a).

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

7 (1) The delivery of the information; or

8 (2) The resolution of any proceedings, including appeals
9 of any proceeding, concerning the State's subpoena or
10 court order.

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

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

18 (2) Has not initiated proceedings to challenge the request
19 of the governmental entity.

20 (e) A governmental entity may seek to require the creation
21 of a backup copy under subsection (a) if, in its sole
22 discretion, the entity determines that there is reason to



1 believe that notification under section 803-P of the existence
2 of the subpoena or court order may result in destruction of or
3 tampering with evidence. This determination is not subject to
4 challenge by the subscriber, customer, or service provider.

5 (f) Within fourteen days after notice by the governmental
6 entity to the subscriber or customer under subsection (b), the
7 subscriber or customer may file a motion to quash the subpoena
8 or vacate the court order, with copies served upon the
9 governmental entity and with written notice of the challenge to
10 the service provider. A motion to vacate a court order shall be
11 filed with the designated judge who issued the order. A motion
12 to quash a subpoena shall be filed in the appropriate court.
13 The motion or application shall contain an affidavit or sworn
14 statement:

15 (1) Stating that the applicant is a customer or subscriber
16 to the service from which the contents of electronic
17 communications maintained for applicant have been
18 sought; and

19 (2) Stating the applicant's reasons for believing that the
20 records sought are not relevant to a legitimate law
21 enforcement inquiry or that there has not been



1 substantial compliance with this part in some other
2 respect.

3 (g) Service shall be made under this section upon a
4 governmental entity by delivering or mailing by registered or
5 certified mail a copy of the papers to the person, office, or
6 department specified in the notice which the customer has
7 received pursuant to this subpart. For the purposes of this
8 section, the term "delivery" shall have the same meaning given
9 to that term in the Hawaii rules of civil procedure.

10 (h) If the court finds that the subscriber or customer has
11 complied with subsection (f)(1) and (2), the court shall order
12 the governmental entity to file a sworn response, which may be
13 filed in camera if the governmental entity includes in its
14 response the reasons that make in camera review appropriate. If
15 the court is unable to determine the motion or application on
16 the basis of the parties' initial allegations and response, the
17 court may conduct additional proceedings as it deems
18 appropriate. All proceedings shall be completed and the motion
19 or application decided as soon as practicable after the filing
20 of the governmental entity's response.

21 (i) If the court finds that the applicant is not the
22 subscriber or customer for whom the communications sought by the



1 governmental entity are maintained, or that there is a reason to
2 believe that the law enforcement inquiry is legitimate and that
3 the communications sought are relevant to that inquiry, it shall
4 deny the motion or application and order the process enforced.
5 If the court finds that the applicant is the subscriber or
6 customer for whom the communications sought by the governmental
7 entity are maintained and that there is no reason to believe
8 that the communications sought are relevant to a legitimate law
9 enforcement inquiry or that there has not been substantial
10 compliance with this subpart, it shall order the process
11 quashed.

12 (j) A court order denying a motion or application under
13 this section shall not be deemed a final order and no
14 interlocutory appeal may be taken therefrom by the customer.

15 **§803-R Delayed notice.** (a) A governmental entity action
16 under section 803-P(b) may:

17 (1) When a court order is sought, include in the
18 application a request, which the court shall grant,
19 for an order delaying the notification required under
20 section 803-P for a period not to exceed ninety days,
21 if the court determines that there is reason to
22 believe that notification of the existence of the



1 court order may have an adverse result described in
2 paragraph (2); or

3 (2) When an administrative subpoena authorized by statute
4 or a grand jury subpoena is obtained, delay the
5 notification required under section 803-P for a period
6 not to exceed ninety days upon the execution of a
7 written certification of a supervisory official that
8 there is reason to believe that notification of the
9 existence of the subpoena may have an adverse result
10 described in subsection (b).

11 (b) An adverse result for purposes of subsection (a) is:

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

14 (2) Flight from prosecution;

15 (3) Destruction of or tampering with evidence;

16 (4) Intimidation of potential witnesses; or

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

19 (c) The governmental entity shall maintain a true copy of
20 certification under subsection (a). Extensions of the delay of
21 notification provided in section 803-P of up to ninety days each
22 may be granted by the court upon application, or by



1 certification by a governmental entity, but only in accordance
2 with subsection (f).

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

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

10 (2) Informs the customer or subscriber:

11 (A) Information maintained for the customer or
12 subscriber by the service provider named in the
13 process 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) Notification to the customer or subscriber was
17 delayed;

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

21 (D) The provision of this part that authorized the
22 delay.



1 (e) As used in this section, the term "supervisory
2 official" means the attorney general, the first deputy attorney
3 general, the prosecuting attorney or the first deputy
4 prosecuting attorney of the applicable county, or the chief of
5 police or the deputy chief of police of the applicable county.

6 (f) A governmental entity acting under section 803-P is
7 not required to notify the subscriber or customer under section
8 803-P(b), or to the extent that it may delay notice pursuant to
9 subsection (a), may apply to a district court judge or a
10 designated judge for an order commanding a provider of
11 electronic communications service or remote computing service to
12 whom a warrant, subpoena, or court order is directed, for such
13 period as the court deems appropriate, not to notify any other
14 person of the existence of the warrant, subpoena, or court
15 order. The court shall enter the order if it determines that
16 there is reason to believe that notification of the existence of
17 the warrant, subpoena, or court order will result in:

- 18 (1) Endangering the life or physical safety of an
19 individual;
- 20 (2) Flight from prosecution;
- 21 (3) Destruction of or tampering with evidence;
- 22 (4) Intimidation of potential witnesses; or



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

3 **§803-S Cost reimbursement.** (a) Except as otherwise
4 provided in subsection (c), a governmental entity obtaining the
5 contents of communications, records, or other information under
6 section 803-O, 803-P, or 803-Q shall pay to the person or entity
7 assembling or providing the information a fee for reimbursement
8 or costs that are reasonably necessary and that have been
9 directly incurred in searching for, assembling, reproducing, or
10 otherwise providing the information. The reimbursable costs
11 shall include any costs due to necessary disruption of normal
12 operations of any electronic communication service or remote
13 computing service in which the information may be stored.

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



1 (c) The requirement of subsection (a) does not apply with
2 respect to records or other information maintained by a
3 communication common carrier that relate to telephone toll
4 records and telephone listings obtained under section 803-P.
5 However, the court may order a payment as described in
6 subsection (a), if the court determines the information required
7 is unusually voluminous in nature or otherwise caused an undue
8 burden on the provider.

9 **§803-T Civil action.** (a) Except as provided in section
10 803-P, any provider of electronic communication service,
11 subscriber, or other person aggrieved by any violation relating
12 to this subpart in which the conduct constituting the violation
13 is engaged in with a knowing or intentional state of mind, may
14 recover such relief as may be appropriate, in a civil action,
15 from the person or entity that engaged in that violation.

16 (b) In a civil action under this section, appropriate
17 relief includes:

- 18 (1) Preliminary and other equitable or declaratory relief
19 as may be appropriate;
- 20 (2) Damages under subsection (c); and
- 21 (3) A reasonable attorney's fee and other litigation costs
22 reasonably incurred.



1 (c) The court may assess as damages in a civil action
2 under this section the sum of the actual damages suffered by the
3 plaintiff and any profits made by the violator as a result of
4 the violation, but in no case shall a person entitled to recover
5 receive less than the sum of \$1,000. If the violation is
6 knowing or intentional, the court may assess punitive damages.
7 In the case of a successful action to enforce liability under
8 this section, the court may assess the costs of the action, in
9 addition to reasonable attorney's fees determined as by the
10 court.

11 (d) If a court determines that any state or county agency
12 or department has violated this subpart and the court finds that
13 the circumstances surrounding the violation raise the question
14 whether an officer or employee of the state or county agency or
15 department acted knowingly or intentionally with respect to the
16 violation, the agency or department concerned shall promptly
17 initiate a proceeding to determine whether disciplinary action
18 is warranted against the officer or employee.

19 (e) It is a complete defense to any civil or criminal
20 action brought pursuant to this subpart or any other law for
21 good faith reliance on:



1 (1) A court warrant or order, a grand jury subpoena, a
2 legislative authorization, or a statutory
3 authorization;

4 (2) A request of an investigative or law enforcement
5 officer under section 803-J(d); or

6 (3) A good faith determination that section 803-B(c)
7 permitted the conduct complained of.

8 (f) A civil action under this section shall not be
9 commenced later than two years after the date upon which the
10 claimant first discovered or had a reasonable opportunity to
11 discover the violation.

12 **§803-U Exclusivity of remedies.** The remedies and
13 sanctions described in this subpart are the only judicial
14 remedies and sanctions for nonconstitutional violations of this
15 subpart.

16 D. MOBILE TRACKING DEVICES

17 **§803-V Application for authorization to install and use a**
18 **mobile tracking device.** (a) A designated judge may issue a
19 warrant or other order for the installation of a mobile tracking
20 device. The order may authorize the use of that device within
21 the jurisdiction of the court and outside that jurisdiction, if
22 the device is installed in that jurisdiction.



1 (b) If, upon application to the designated judge for a
2 court order, the designated judge finds that there are
3 sufficient facts and circumstances contained within the
4 application to establish probable cause to believe that the use
5 of a mobile tracking device will discover the fruits,
6 instrumentalities, or evidence of a crime or is relevant to an
7 ongoing criminal investigation, the designated judge shall
8 proceed under subsection (c).

9 (c) If the designated judge makes the findings under
10 subsection (b), the designated judge shall issue an order
11 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 locations where the devices are to be
16 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 the
22 orders may be granted only upon reapplication establishing



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

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

6 **§803-W Prohibited use of a pen register or a trap and**

7 **trace device.** (a) A person, not excluded by subsection (b),
8 commits the offense of prohibited use of a pen register or a
9 trap and trace device if the person installs or uses a pen
10 register or a trap and trace device without first obtaining a
11 court order under section 803-Y.

12 (b) Subsection (a) does not apply with respect to the use
13 of a pen register or a trap and trace device by a provider of
14 electronic or wire communication service:

15 (1) Relating to the operation, maintenance, and testing of
16 a wire or electronic communication service or to the
17 protection of the rights or property of the provider
18 or to the protection of users of that service from
19 abuse of service or unlawful use of service;

20 (2) To record the fact that a wire or electronic
21 communication was initiated or completed in order to
22 protect the provider, another provider furnishing



1 service toward the completion of the wire
2 communication, or a user of that service from
3 fraudulent, unlawful, or abusive use of service; or
4 (3) Where the consent of the user of that service has been
5 obtained.

6 (c) A government agency authorized to install and use a
7 pen register under this subpart shall use technology reasonably
8 available to it that restricts the recording or decoding of
9 electronic or other impulses to the dialing and signaling
10 information utilized in call processing.

11 (d) Prohibited use of a pen register or a trap and trace
12 device is a misdemeanor.

13 **§803-X Application for an order for a pen register or a**
14 **trap and trace device.** (a) The attorney general or the
15 prosecuting attorney for each county, or their designees, or an
16 investigative or law enforcement officer may make application,
17 in writing under oath or equivalent affirmation, to a designated
18 judge for an order or an extension of an order issued under
19 section 803-Y authorizing or approving the installation and use
20 of a pen register or a trap and trace device under this subpart.

21 (b) The application required under subsection (a) shall
22 include:



1 (1) The identity of the official or the investigative or
 2 law enforcement officer making the application and the
 3 identity of the law enforcement agency conducting the
 4 investigation; and

5 (2) A certification by the applicant that the information
 6 likely to be obtained is relevant to an ongoing
 7 criminal investigation being conducted by that agency.

8 **§803-Y Issuance of an order for a pen register or a trap**
 9 **and trace device.** (a) Upon an application made under section
 10 803-X, the court shall enter an ex parte order authorizing the
 11 installation and use of a pen register or a trap and trace
 12 device within the jurisdiction of the court, if the court finds
 13 there are sufficient facts and circumstances contained within
 14 the application to establish probable cause to believe that the
 15 information to be obtained will constitute fruits, instruments,
 16 or evidence of a crime or is relevant to an ongoing criminal
 17 investigation.

18 (b) An order issued under this section:

19 (1) Shall specify:

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

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

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

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

11 (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 (2) Shall direct, upon the request of the applicant, the
15 furnishing of information, facilities, and technical
16 assistance necessary to accomplish the installation of
17 the pen register or trap and trace device under
18 section 803-Z.

19 (c) An order issued under this subpart shall authorize the
20 installation and use of a pen register or a trap and trace
21 device for a period not to exceed sixty days. Extensions of an
22 order may be granted, but only upon an application for an order



1 under section 803-X and upon the judicial finding required by
2 subsection (a). The period of extension shall be for a period
3 not to exceed sixty days.

4 (d) An order authorizing or approving the installation and
5 use of a pen register or a trap and trace device shall direct
6 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 a trap and trace device is attached, or
11 who has been ordered by the court to provide
12 assistance to the applicant, not disclose the
13 existence of the pen register or trap and trace device
14 or the existence of the investigation to the listed
15 subscriber or to any other person, unless or until
16 otherwise ordered by the court.

17 **§803-Z Assistance in installation and use of a pen**
18 **register or a trap and trace device.** (a) Upon the request of
19 the attorney general or the county prosecuting attorney, or
20 their designees, or an investigative or law enforcement officer
21 authorized to install and use a pen register under this subpart,
22 a provider of wire or electronic communication service,



1 landlord, custodian, or other person shall furnish the
2 investigative or law enforcement officer all information,
3 facilities, and technical assistance necessary to accomplish the
4 installation of the pen register unobtrusively and with a
5 minimum of interference with the services that the person so
6 ordered by the court accords the party with respect to whom the
7 installation and use is to take place, if the assistance is
8 directed by a court order as provided in section 803-Y(b)(2).

9 (b) Upon the request of the attorney general or the county
10 prosecuting attorney, or a designee, or an officer of a law
11 enforcement agency authorized to receive the results of a trap
12 and trace device under this subpart, a provider of a wire or
13 electronic communication service, landlord, custodian, or other
14 person shall install the device as soon as practicable on the
15 appropriate line and shall furnish the investigative or law
16 enforcement officer all additional information, facilities, and
17 technical assistance including installation and operation of the
18 device unobtrusively and with a minimum of interference with the
19 services that the person so ordered by the court accords the
20 party with respect to whom the installation and use is to take
21 place, if the installation and assistance is directed by a court
22 order as provided in section 803-Y(b)(2). Unless otherwise



1 ordered by the court, the results of the trap and trace device
2 shall be furnished, pursuant to section 803-Y(b) or 803-AA, to
3 the officer of a law enforcement agency, designated in the court
4 order, at reasonable intervals during regular business hours for
5 the duration of the order.

6 (c) A provider of a wire or electronic communication
7 service, landlord, custodian, or other person who furnishes
8 facilities or technical assistance pursuant to this section
9 shall be reasonably compensated for the reasonable expenses
10 incurred in providing the facilities and assistance.

11 (d) No cause of action shall lie in any court against any
12 provider of a wire or electronic communication service, its
13 officers, employees, agents, or other specified persons for
14 providing information, facilities, or assistance in accordance
15 with the terms of a court order under this part or requested
16 pursuant to section 803-AA.

17 (e) A good faith reliance on a court order under this
18 part, a request pursuant to section 803-AA, a legislative
19 authorization, or a statutory authorization is a complete
20 defense against any civil or criminal action brought under this
21 subpart or any other law.



1 **§803-AA Reports concerning pen registers and trap and**
2 **trace devices.** The attorney general, at least twenty days prior
3 to the convening of each regular session, shall annually report
4 to the legislature on the number of pen register orders and
5 orders for trap and trace devices applied for by law enforcement
6 agencies of the State."

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

9 "**§641-13 By State in criminal cases.** An appeal may be
10 taken by and on behalf of the State from the district or circuit
11 courts to the supreme appellate court, subject to chapter 602,
12 in all criminal cases, in the following instances:

13 (1) From an order or judgment quashing, setting aside, or
14 sustaining a motion to dismiss[7] any indictment,
15 information, or complaint or any count thereof;

16 (2) From an order or judgment[7] sustaining a special plea
17 in bar[7] or dismissing the case where the defendant
18 has not been put in jeopardy;

19 (3) From an order granting a new trial;

20 (4) From an order arresting judgment;



- 1 (5) From a ruling on a question of law adverse to the
2 State, where the defendant was convicted and appeals
3 from the judgment;
- 4 (6) From the sentence, on the ground that it is illegal;
- 5 (7) From a pretrial order granting a motion for the
6 suppression of evidence, including a confession or
7 admission, or the return of property, in which case
8 the intermediate appellate court or the supreme court,
9 as the case may be, shall give priority to [~~such an~~
10 the appeal and the order shall be stayed pending the
11 outcome of the appeal;
- 12 (8) From an order denying a request by the State for
13 protective order for nondisclosure of witness for
14 [~~their~~] reason of personal safety under Rule 16(e) (4)
15 of the Hawaii Rules of Penal Procedure, in which case
16 the intermediate appellate court shall give priority
17 to [~~such~~] the appeal and the order shall be stayed
18 pending outcome of [~~such~~] the appeal; [~~or~~]
- 19 (9) From a judgment of acquittal following a jury verdict
20 of guilty[~~-~~]; and
- 21 (10) From a denial of an application for an order of
22 approval or authorization of the interception of a

1 wire, oral, or electronic communication pursuant to
2 section 803-H."

3 SECTION 3. Part IV of chapter 803, Hawaii Revised
4 Statutes, is repealed.

5 SECTION 4. In codifying the new part added to chapter 803,
6 Hawaii Revised Statutes, by section 1 of this Act, the revisor
7 of statutes shall substitute appropriate section numbers for the
8 letters used in the new sections' designations in this Act.

9 SECTION 5. This Act does not affect rights and duties that
10 matured, penalties that were incurred, and proceedings that were
11 begun, before its effective date.

12 SECTION 6. Statutory material to be repealed is bracketed
13 and stricken. New statutory material is underscored.

14 SECTION 7. This Act shall take effect on June 30, 2006;
15 provided that the amendments made to section 641-13, Hawaii
16 Revised Statutes, by section 2 of this Act shall not be repealed
17 when section 70 of Act 202, Session Laws of Hawaii 2004, takes
18 effect on July 1, 2006.

Bob Hogue

April Y. J. Perreault

INTRODUCED BY:

Anna Iwamoto

Clarence K. ...
Will ...

[Signature]

Maaine R. ...

Russell Kohl



Theranne Chun Oakland

Norman Sakamoto

SB. NO. 2978

Report Title:

Electronic Surveillance; Wiretapping; Conformance to Federal Law

Description:

Repeals State's electronic surveillance statute and conforms the State's electronic surveillance laws to federal laws; regulates oral, electronic, and wire communications surveillance and interception; sets procedures for surveillance and interception.

