POLICE DEPARTMENT

CITY AND COUNTY OF HONOLULU

801 SOUTH BERETANIA STREET · HONOLULU, HAWAII 96813
TELEPHONE: (808) 529-3111 · INTERNET: www.honolulupd.org

RICK BLANGIARDI
MAYOR

RADE K. VANIC
INTERIM CHIEF

OUR REFERENCE JH-KK

March 15, 2022

The Honorable Mark M. Nakashima, Chair
and Members
Committee on Judiciary and
Hawaiian Affairs
House of Representatives
Hawaii State Capitol
415 South Beretania Street, Room 325
Honolulu, Hawaii 96813

Dear Chair Nakashima and Members:

SUBJECT: Senate Bill No. 2291, Relating to Electronic Eavesdropping

I am Jarod Hiramoto, Captain of the Criminal Investigation Division of the Honolulu Police Department (HPD), City and County of Honolulu.

The HPD supports Senate Bill No. 2291, Relating to Electronic Eavesdropping. With the United States Supreme Court ruling in Carpenter versus the United States, it is essential that the Hawaii Revised Statutes be amended to be consistent with the requirements for law enforcement to seek search warrants to review records.

The HPD urges you to support Senate Bill No. 2291, Relating to Electronic Eavesdropping, and thanks you for the opportunity to testify.

APPROVED:

Rade K. Vanic
Interim Chief of Police

Sincerely,

Jarod Hiramoto, Captain
Criminal Investigation Division

DEPARTMENT OF THE PROSECUTING ATTORNEY

CITY AND COUNTY OF HONOLULU

ALII PLACE
1060 RICHARDS STREET • HONOLULU, HAWAII 96813
PHONE: (808) 768-7400 • FAX: (808) 768-7515

STEVEN S. ALM
PROSECUTING ATTORNEY

THOMAS J. BRADY
FIRST DEPUTY
PROSECUTING ATTORNEY

THE HONORABLE MARK M. NAKASHIMA, CHAIR
HOUSE COMMITTEE ON JUDICARY AND HAWAIIAN AFFAIRS
Thirty-First State Legislature
Regular Session of 2022
State of Hawai`i

March 15, 2022

RE: S.B. 2291; RELATING TO ELECTRONIC EAVESDROPPING.

Chair Nakashima, Vice Chair Matayoshi, and members of the Committee on Judiciary and Hawaiian Affairs, the Department of the Prosecuting Attorney, City and County of Honolulu ("Department"), submits the following testimony in **strong support** of S.B. 2291.

S.B. 2291 is the product of the Twenty-First Century Privacy Law Task Force ("Task Force"). The Task Force was created as a result of House Concurrent Resolution No. 225 of the 2019 Legislature. Through HCR 225, the Legislature found that "public interest usage has significantly expanded in recent years and that a lack of meaningful government regulation has resulted in the privacy of individuals being compromised. Accordingly, the Legislature asked for an examination existing privacy laws and regulations to determine how to protect the privacy interests of the people of Hawaii while meeting or exceeding the existing privacy protections established in the State Constitution and Hawaii Revised Statutes". [1]

The Task Force was Chaired by then Representative, now Senator, Chris Lee, and Co-Chaired by Senator Michelle Kidani. Task Force members included attorneys from the State Attorney General's Office, the Department of Commerce and Consumer Affairs, the Honolulu Department of the Prosecuting Attorney, and the ACLU-Hawaii, as well as the State of Hawaii's Chief Information Officer. The Task Force also included experts from the private sector, such as Charter Communications, Think Tech Hawaii, Pono Media, and certified privacy experts. The Task Force received numerous presentations, including presentations from the ACLU-Hawaii, the Honolulu Police Department, privacy law experts, and communication service providers.

S.B. 2291 was unanimously adopted and approved by every member of the Task Force, including the State of Hawaii Attorney General's Office.

[1] Report to the Legislature, House Concurrent Resolution N. 225, HD1, SD1 (2019), Twenty-First Century Privacy Law Task Force, p. 5., submitted to the Legislature on February 5, 2020.

The purpose of S.B. 2291 is to make it clear that law enforcement must use a search warrant to obtain access to electronically stored data, regardless of how that data is classified. Currently, Hawaii law permits law enforcement to obtain access to electronically stored data using one of three forms of legal process: (1) a "subpoena" (for subscriber/account records), (2) a "court order" (for historical transactional records, such as cell site data), and (3) a "search warrant" (for "content" such as e-mail and text messages). The evidentiary burden to use a subpoena and court order is lower than the burden imposed by a search warrant. Whereas the burden to use a subpoena and court order is "materiality" and "relevance", the burden to obtain a search warrant requires that law enforcement establish "probable cause that the data to be seized constitutes evidence of a crime". That is a higher burden of proof. It requires specificity, and it invokes all of the constitutional protections that attach to a search warrant. Requiring that law enforcement use a search warrant to obtain access to electronically stored data will provide greater protection to Hawaii residents who are the subject of a law enforcement investigation.

S.B. 2291 advances the primary objective of HCR 225: To "protect the privacy interests of the people of Hawaii while meeting or exceeding the existing privacy protections established in the State Constitution and Hawaii Revised Statutes". The people of the State of Hawaii have a constitutional "right to privacy". That right is enshrined in article I, section 6 of the Hawaii Constitution. Article I, section 6 is entitled "Searches, Seizures, and Invasion of Privacy". S.B. 2291 honors the Hawaii Constitution, and it meets the minimal expectations that Hawaii residents have about the privacy of their information – that it will be protected against disclosure absent a search warrant issued by a neutral judge.

The following is a breakdown of the various sections of S.B. 2291.

Section 3, Pg. 3 – 7. This section governs law enforcement's authority to compel disclosure of various forms of information stored by "electronic communication services" (such as Google, Apple, Microsoft, Verizon, Hawaiian Telcom, Spectrum, Facebook, and others) and "remote computing services" (such as web hosting companies and cloud-based storage providers like Dropbox). Currently, if law enforcement wants to compel disclosure of the "contents" of communications (such as e-mail, text messages, or private "comments or tweets"), law enforcement must obtain a search warrant. If law enforcement wants to compel disclosure of "transactional records" (such as IP logs, cell site data, and e-mail headers), law enforcement must obtain a court order. If law enforcement wants to compel disclosure of call detail records, or subscriber or account user information, law enforcement is permitted to use a subpoena. S.B. 2291 eliminates the disparate treatment between "content", "transactional records", and "account user" records, and treats all forms of electronically stored data the same, namely they receive the same protection against disclosure. Thus, if S.B. 2291 is enacted, law enforcement would be required to obtain a search warrant (from a neutral judge) before accessing any form of electronically stored data from "electronic communication services" and "remote computing services", or they must obtain the consent of the subscriber, customer, or user of the service.

The statutes to be amended by S.B. 2291, as they exists right now, are inconsistent with important case law. For example, HRS Section 803-47.6(d)(2)(D), as it exists right now, authorizes law enforcement to use a court order to obtain "transactional records", (such as IP logs, cell site data, and e-mail headers). However, the U.S. Supreme Court ruled in 2018 in the case of *Carpenter v. United States* that a search warrant – not a court order – was required to compel the production of cell site data. In addition, in 2014, the Hawaii Supreme Court issued an opinion in the case of *State v. Walton*. In that case, the Court overruled 35 years of precedent when they invalidated the "third-party records doctrine". The *Walton* case made two things crystal clear to experienced,

knowledgeable prosecutors: (1) if prosecutors attempt to use a subpoena or court order – as opposed to a search warrant – to compel the production of records, the Hawaii Supreme Court will not only invalidate that procedure but also invalidate the statutes sought to be amended by S.B. 2291, and (2) the Hawaii Supreme Court will find that the people of Hawaii have a constitutional right to privacy, enshrined in article I, section 6 of the Hawaii State Constitution, against disclosure absent the issuance of a search warrant signed by a neutral judge.

Section 4, Pg. 7 – 9. This section relates to "court orders" granted at the request of law enforcement that order "electronic communication services" and "remote computing services" to make a "backup" of an online account. Since the proposal to Section 803-47.6, Hawaii Revised Statutes, will require that law enforcement obtain a "search warrant" (instead of a "court order"), the proposed change simply replaces the "court order" language with "search warrant" language.

Section 8, Pg. 9 – 11. This section relates to scenarios when the court can delay disclosure to a user. In practice, Hawaii courts grant delayed disclosure in nearly all cases involving law enforcement's access to online data. Court-approved non-disclosure orders are based on the need to prevent the harms set forth in HRS §803-47.8(e). In practice, law enforcement discloses their access to records as part of the discovery process in criminal cases. The discovery materials, including copies of the legal process and the records obtained, are provided in discovery to defense counsel and the defendant within 10 days of arraignment, pursuant to Rule 16 of the Hawaii Rules of Penal Procedure (HRPP). The proposal to HRS §803-47.8 would retain the judicial discretion provision, and require that disclosure be made no later than the deadline for providing discovery in a criminal case – 10 days after arraignment.

Section 2, Pg. 2 – 3. This section relates to a proposed amendment to HRS §803-41 (the definition section), to update the definition of "electronically stored data". The Task Force unanimously agreed that "electronically stored data" would be defined as "any information that is recorded, stored, or maintained in electronic form by an electronic communication service or a remote computing service, and includes, but is not limited to, the contents of communications, transactional records about communications, and records and information that relate to a subscriber, customer, or user of an electronic communication service or a remote computing service." Thus, it will provide a clear definition for the proposed language in HRS §803-47.7.

For all of the foregoing reasons, the Department of the Prosecuting Attorney of the City and County of Honolulu supports the passage of S.B. 2291. Thank you for the opportunity to testify on this matter.

DAVID Y. IGE
GOVERNOR

JOSH GREEN
LT. GOVERNOR

STATE OF HAWAII
OFFICE OF THE DIRECTOR
DEPARTMENT OF COMMERCE AND CONSUMER AFFAIRS
335 MERCHANT STREET, ROOM 310
P.O. BOX 541
HONOLULU, HAWAII 96809
Phone Number: 586-2850
Fax Number: 586-2856
cca.hawaii.gov

CATHERINE P. AWAKUNI COLÓN
DIRECTOR

JO ANN M. UCHIDA TAKEUCHI
DEPUTY DIRECTOR

Testimony of the Department of Commerce and Consumer Affairs

Before the
House Committee on Judiciary & Hawaiian Affairs
Tuesday, March 15, 2022
2:00 p.m.
Via Videoconference

On the following measure:
S.B. 2291, RELATING TO ELECTRONIC EAVESDROPPING

Chair Nakashima and Members of the Committee:

My name is Catherine P. Awakuni Colón, and I am the Director of the Department of Commerce and Consumer Affairs (Department). The Department has concerns about this bill to the extent it may impact the Department's ability to obtain electronic records and as such opposes this bill in its current form.

The purposes of this bill are to: (1) amend provisions relating to electronic eavesdropping; (2) require law enforcement entities to obtain a search warrant before accessing a person's electronic communications in certain circumstances and (3) amend notification requirements of a law enforcement entity's access to electronic communications to allow for discovery in criminal cases.

Civil Enforcement Authority. The Department has broad authority under Haw. Rev. Stat. §26-9(j) to investigate matters within its jurisdiction, including subpoena authority. In addition, several divisions within the Department have specific authority to subpoena records relevant to division-specific investigations. While the Department has not historically viewed Ch. 803 Haw. Rev. Stat. as applicable to its civil subpoena

authority, the sweeping language of this bill raises concerns that the bill creates ambiguity as to its applicability to civil enforcement actions. To avoid unnecessary confusion, the Department believes that it should be clear that the language of the SB 2291 only applies to obtaining electronically stored data in criminal investigations and not to civil enforcement actions. In this regard, the Department respectfully requests that the committee report reflect that any amendments to section 803-46.6 Haw. Rev. Stats. only apply to criminal search warrants and not to the Department's authority to issues civil administrative subpoenas.

Criminal Enforcement Authority. The Department's Insurance Fraud branch investigates and prosecutes insurance fraud through its criminal enforcement authority. The Department defers to the Department of the Attorney General regarding the impact this bill may have on criminal enforcement matters.

Thank you for the opportunity to testify on this bill.

TESTIMONY OF
THE DEPARTMENT OF THE ATTORNEY GENERAL
THIRTY-FIRST LEGISLATURE, 2022

ON THE FOLLOWING MEASURE:
S.B. NO. 2291, RELATING TO ELECTRONIC EAVESDROPPING.

BEFORE THE:
HOUSE COMMITTEE ON JUDICIARY AND HAWAIIAN AFFAIRS

DATE: Tuesday, March 15, 2022 **TIME:** 2:00 p.m.

LOCATION: State Capitol, Room 325, Via Videoconference

TESTIFIER(S): Holly T. Shikada, Attorney General,
Thomas Berger, Deputy Attorney General,
Bryan C. Yee, Deputy Attorney General, or
Albert Cook, Deputy Attorney General

Chair Nakashima and Members of the Committee:

The Department of the Attorney General (Department) opposes this bill based on the Attorney General's role as the Chief Law Enforcement Officer for the State of Hawai‘i.

This bill removes the ability of criminal law enforcement entities to obtain electronically stored data, specifically, subscriber information and transactional records from electronic communication services (ECS) and remote computing services (RCS) by use of a court order or administrative subpoena, instead requiring a search warrant for all electronically stored data. It also requires criminal law enforcement entities to immediately notify the subscriber, customer, or user of the ECS or RCS that the government agencies have received information from an ECS or RCS, unless they receive permission of a court to extend the notification for 90 days or until the discovery deadline in a criminal case.

The stated intended purpose of this bill is to align state statutes with the holding by the Supreme Court in *Carpenter v. United States,* 138 S. Ct. 2206 (2018), and with current law enforcement practice. However, this bill goes beyond the requirements in *Carpenter*.

In *Carpenter*, the Supreme Court held that the "Government's acquisition of the cell-site records" without obtaining a search warrant "was a search within the meaning

of the Fourth Amendment." 136 S. Ct. at 2220. And, "the Government must generally obtain a warrant supported by probable cause before acquiring such records." *Id.* at 2221. The holding in *Carpenter* was expressly limited by the Supreme Court to collection by law enforcement of cell-site location information: "Our decision today is a narrow one. We do not express a view on matters not before us[.]" 136 S. Ct. at 2220.

This bill requires a search warrant for much more than cell-site location information. Section 3 of this bill, on page 3, lines 7-12, amends section 803-47.8, Hawaii Revised Statutes (HRS), to require a search warrant for not only cell-site records, but also for any "electronically stored data." Moreover, section 2 of this bill on page 2, line 15, to page 3, line 4, amends section 803-41, HRS, to broadly define "electronically stored data" as "any information that is recorded, stored, or maintained in electronic form by an electronic communication service or a remote computing service." Consequently, this bill requires a search warrant for even basic subscriber information such as an internet protocol address, an e-mail address, or a telephone number. Although civil governmental entities have other authority to obtain electronic stored data, criminal law enforcement entities do not. This bill, therefore, would impede the ability of law enforcement to investigate crimes involving electronically stored data, including internet crimes against children.

Current Hawai‘i statutes comply with the Electronic Communications Privacy Act (ECPA) 18 U.S.C. sections 2510 to 2523 and 18 U.S.C. sections 2701 to 2712. The ECPA already provides the generally accepted statutory framework governing access by the government to stored electronic communications, while protecting individual privacy. In addition, this bill is unnecessary to conform to the holding in *Carpenter* because that decision is already applicable to law enforcement and any amendment to the statutes is not necessary.

We, therefore, request the measure be held to avoid an unnecessary impediment to protecting the public from crime.

In the event the Committee is inclined to pass the measure, the Department requests the bill include the following amendments.

First, the Department requests the following amendments to clarify that the measure only applies to criminal law enforcement entities, and does not take away any authority from civil enforcement authorities from protecting the public:

> In the preamble, on page 2, line 3, insert the word "criminal" after the word "Require" and before the phrase "law enforcement." The amended bill would read on page 2, line 3, "(1) Require criminal law enforcement . . . ."
>
> In section 3, for the amendment to section 803-47.6(a), HRS, on page 3, line 8, delete the phrase "governmental entity" and insert the phrase "criminal law enforcement officer". The amended bill would read on page 3, line 8, "Except as otherwise provided by law, a [~~governmental entity~~] criminal law enforcement officer may . . . ."

Second, the Department requests the following amendment to make the substance of the bill more consistent with its stated intent to conform Hawaii law to the *Carpenter* decision by ensuring that law enforcement officials continue to have the authority to utilize subpoenas to obtain certain limited information concerning electronic communication (but not including the contents of the electronic communication) consistent with the *Carpenter* decision and existing practice:

> In section 3, add a proviso to section 803-47.6, HRS, at page 3, line 14, with the following wording:
> ". . . user of the service; provided that a provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to, or customer of,

> the service (other than the contents of an electronic communication) to a governmental entity when presented with an administrative subpoena authorized by statute, an attorney general subpoena, or a grand jury or trial subpoena, which seeks the disclosure of information concerning electronic communication, including but not limited to the name, address, local and long distance telephone billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of the service and the types of services the subscriber or customer utilized. A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer."

Finally, the Department requests an amendment to delete the proposed section 803-47.6(b), HRS, which requires that criminal law enforcement notify a suspect when receiving records or information whether obtained by a search warrant or a subpoena. Such a requirement is not required by the *Carpenter* decision, is not consistent with existing law enforcement practice, and would place the burden on criminal law enforcement to notify a suspect of an ongoing investigation and could compromise the investigation or result in destruction of evidence. The requested amendment is as follows:

> In section 3, at page 6, lines 14-17, delete the proposed section 803-47.6(b), HRS.

We respectfully request that this measure be held. If the bill is not to be held, we request that the measure include the clarifying amendments.

Rebecca Like
Acting Prosecuting Attorney

Jennifer S. Winn
Acting First Deputy

Leon J. C. Davenport, III
Acting Second Deputy

Diana Gausepohl-White
Victim/Witness Program Director

Theresa Koki
Life's Choices Kaua'i Program
Prevention Services Coordinator

OFFICE OF THE PROSECUTING ATTORNEY
County of Kaua'i, State of Hawai'i
3990 Ka'ana Street, Suite 210, Līhu'e, Hawai'i 96766
808-241-1888 ~ FAX 808-241-1758
Victim/Witness Program 808-241-1898 or 800-668-5734

March 14, 2022

RE: SB 2291; RELATING TO ELECTRONIC EAVESDROPPING

Chair Rhoads, and members of the Senate Committee on the Judicary, the Office of the Prosecuting Attorney of the County of Kauai ("OPA") submits the following testimony in opposition of S.B. 2291.

The Office of the Prosecuting Attorney of the County of Kauai concurs with the testimony given by the Attorney General that State law is already in compliance with *Carpenter* and does not need to be amended.

In the early stages of an investigation law enforcement frequently has just a phone number as an identifier for messages sent to a victim. Requiring our law enforcement partners to obtain a search warrant to obtain subscriber information from a cellular carrier is unduly burdensome and will make their investigations less efficient. Revealing subscriber information is completely different from the situation in *Carpenter* where law enforcement had obtained cell-site location information(which law enforcement can then use to create a map of where the phone and presumably the suspect had travelled) that the suspect had a reasonable expectation of privacy in. Allowing law enforcement to quickly identify who the subscriber is will allow them to focus their investigation, identify the owner of the cell phone used to send an illicit message, and obtain a search warrant for the contents of the cell phone before it is potentially thrown away or destroyed by the suspect.

In addition, the requirements of this bill would in some circumstances make it impossible for law enforcement to identify the suspect.

For these reasons, the Office of the Prosecuting Attorney of the County of Kauai opposes the passage of S.B. 2291 and respectfully request that this measure be held. Thank you for the opportunity to testify on this matter.

POLICE DEPARTMENT
COUNTY OF KAUAI

DEREK S.K. KAWAKAMI, MAYOR
MICHAEL A. DAHILIG, MANAGING DIRECTOR

TODD G. RAYBUCK, CHIEF OF POLICE
STAN R. OLSEN, DEPUTY CHIEF OF POLICE

Testimony of James Miller
A\Captain
Kauai Police Department

Before the
Committee on Public Safety,
Committee on Judiciary & Hawaiian Affairs
March 15, 2022, 2:00 pm
via Videoconference

In consideration of
Senate Bill 2291
Relating to Law Enforcement

Chair Nakashima, Vice-Chair Matayoshi and members of the House Committee on Judiciary and Hawaiian Affairs, the Kauai Police Department submits the following testimony **IN OPPOSITION to S.B. 2291.** Thank you for the opportunity to be heard on this matter.

The Kauai Police Department (KPD) is in support of the Kauai County Office of the Prosecuting Attorney and the Office of the Attorney General in **opposing** Senate Bill 2291, Relating to law enforcement, requiring a search warrant instead of a subpoena to obtain subscriber information for investigations.

In the initial stages of investigations such as those involving cell phones where text messages and images of an inappropriate nature are sent to a juvenile, most of the time we would only have a phone number to work with. Using just that phone number would not meet the requirements needed to obtain a search warrant for the information required, ending most investigations before they could begin.

In the example given above, without knowing who the subscriber of the phone is, we don't know what the intent of the message was. Was the message sent to the wrong person? Did the sender of the message know that they were sending inappropriate content to a juvenile? This kind of information is needed to apply for a search warrant. By being able to use a subpoena as a starting point, we can obtain the subscriber information and try to answer those questions based on the person identified as the subscriber. Based on that information and the investigation conducted to determine the relationship and the intent of the sender, we would have a basis to apply for a search warrant as needed.

For the foregoing reasons, the Kauai Police Department **opposes** Senate Bill 2291 as written. Thank you for your time and consideration regarding this proposed legislation.