LATE

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:
SENATE COMMITTEE ON JUDICIARY

DATE: Thursday, February 24, 2022 **TIME:** 9:30 a.m.

LOCATION: State Capitol, Via Videoconference

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

Chair Rhoads 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 government 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 government 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 is significantly broader and expands the holding of *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 (CSLI): "Our decision today is a narrow one. We do not express a view on matters not before us[.]" 136 S. Ct. at 2220.

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 more than just cell-site records and requires that a search warrant be used to obtain "electronically stored data." Section 2 of this bill on page 2, line 15, to page, line 4, amends section 803-41, HRS, to add a new definition of "electronically stored data," which is defined broadly to mean "any information that is recorded, stored, or maintained in electronic form by an electronic communication service or a remote computing service." This bill requires a search warrant for not just cell-site records, but also basic subscriber information such as an internet protocol address, an e-mail address, or a telephone number. Such a requirement would impede the ability of law enforcement to investigate crimes involving electronically stored data.

Current Hawaii statutes comply with the Electronic Communications Privacy Act (ECPA) 18 U.S.C. Sections 2510 to 2523. The ECPA already provides the generally accepted statutory framework governing access by the government to stored electronic communications. However, if the intent of the bill is to conform to the holding in *Carpenter*, that decision is already applicable to law enforcement and any amendment to the statutes are not necessary. This is because Supreme Court decisions are precedent applicable to state and federal courts that are presented with the question of whether a search is lawful under the Fourth Amendment of the United States Constitution.

We respectfully request that this measure be held.

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 KARL RHOADS, CHAIR
SENATE COMMITTEE ON JUDICARY
Thirty-First State Legislature
Regular Session of 2022
State of Hawai`i

February 24, 2022

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

Chair Rhoads, Vice Chair Keohokalole, and members of the Senate Committee on Judiciary, the Department of the Prosecuting Attorney, City and County of Honolulu ("Department"), submits the following testimony in **support** of S.B. 2291.

The Department would like to first thank the Legislature for the opportunity to participate as a member of the Twenty-First Century Privacy Law Task Force ("Task Force"). Each member of the Task Force devoted a significant amount of time and effort to the drafting of this bill (and numerous other bills). Our Department would like to commend all the members for their dedication to their work on the Task Force.

The proposal that is set forth in S.B. 2291 was adopted unanimously by all members of the Task Force, including the ACLU who was a member of the Task Force.

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.

Section 3, Pg. 3 – 7. This section governs law enforcement's legal 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. The attached proposal 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 the proposal is adopted, 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. This section is significant, as the proposed amendment will bring Hawaii law in-line with the 2018 U.S. Supreme Court case, *Carpenter v. United States*, which held that a search warrant—not a court order—was required to compel access to cell site data.

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.

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 BM-KK

February 24, 2022

The Honorable Karl Rhoads, Chair
and Members
Committee on Judiciary
State Senate
Hawaii State Capitol
415 South Beretania Street
Honolulu, Hawaii 96813

Dear Chair Rhoads and Members:

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

I am Benjamin Moszkowicz, Major 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,

Benjamin Moszkowicz, Major
Criminal Investigation Division

SB-2291
Submitted on: 2/19/2022 5:56:47 PM
Testimony for JDC on 2/24/2022 9:30:00 AM

Submitted By	Organization	Testifier Position	Remote Testimony Requested
Dara Carlin, M.A.	Individual	Support	No

Comments:

Stand in Support.

February 22, 2022

S.B. 2291 Relating to Electronic Eavesdropping
Senate Committee on Judiciary
Hearing Date/Time: Thursday, February 24, 2022, 9:30 AM

Dear Chair Rhoads, Vice Chair Keohokalole, and members of the Committee:

I write in SUPPORT of S.B. 2291 Relating to Electronic Eavesdropping. As a privacy expert, I have worked in data privacy for over 15 years and served on the 21st Century Privacy Law Task Force created in 2019 by HCR 225.

In recent years, the amount of electronic stored information collected about Americans has grown exponentially. In addition, case law pertaining to this data has continued to evolve. Most notably, the case Capenter v. United States was heard by the US Supreme Court in 2017. In this case, the FBI used a court order, not a warrant, to gain access to a person's cell phone data, including location records. The majority opinion, penned by Chief Justice Roberts, established that this data was sufficiently personal that a court order was an insufficient bar to discovery. It furthermore stipulated that a warrant should be required to access this personal data.

S.B. 2291 brings Hawaii law into alignment with the Supreme Court decision in Capenter v. United States, requiring a warrant rather than a court order to obtain electronically stored communication data.

Thank you for your consideration and the opportunity to support this legislation.

Kelly McCanlies

Kelly McCanlies
Fellow of Information Privacy, CIPP/US, CIPM, CIPT