LATE

DEPARTMENT OF THE PROSECUTING ATTORNEY

CITY AND COUNTY OF HONOLULU

ALII PLACE
1060 RICHARDS STREET • HONOLULU, HAWAII 96813
PHONE: (808) 547-7400 • FAX: (808) 547-7515

KEITH M. KANESHIRO
PROSECUTING ATTORNEY

CHASID M. SAPOLU
FIRST DEPUTY PROSECUTING ATTORNEY

THE HONORABLE DONNA MERCADO KIM, CHAIR
SENATE COMMITTEE ON GOVERNMENT OPERATIONS

THE HONORABLE GLENN WAKAI, CHAIR
SENATE COMMITTEE ON ECONOMIC DEVELOPMENT, TOURISM, AND TECHNOLOGY

Twenty-Ninth State Legislature
Regular Session of 2018
State of Hawai`i

February 2, 2018

RE: S.B. 2454; RELATING TO ELECTRONIC EAVESDROPPING.

Chair Mercado Kim, Chair Wakai, Vice Chair Ruderman, Vice Chair Taniguchi and members of the Senate Committee on Government Operations and Economic Development, Tourism, and Technology, the Department of the Prosecuting Attorney for the City and County of Honolulu ("Department") submits the following testimony **in opposition** to S.B. 2454 and offers suggested amendments.

The purpose of S.B. 2454 is to prohibit law enforcement from using a cell site simulator, except in three scenarios: (1) the target consents to the intercept of their cell site data, (2) law enforcement obtains a search warrant, or (3) an exception to the warrant requirement applies. However, even if one of those three exceptions applies, law enforcement must still obtain a written court order before using a cell site simulator. In order to obtain a written court order law enforcement will have to comply with all of the provisions set forth on pages 18 – 25 of the proposed bill. In short, even when an exception applies, law enforcement will still be required to prepare a written application, have that application reviewed by a judge, and persuade the judge to issue a written order that satisfies all of the requirements set forth on page 21-23 of the proposed bill.

The practical effect of S.B. 2454, and specifically the requirements set forth in the amendments to section 803-44.5 and section 803-44.6 of the Hawaii Revised Statutes, will render the use of a cell site simulator useless to law enforcement in scenarios where it is most needed – emergency situations such as when the police are attempting to locate or rescue a kidnapped child, or when they're attempting to locate a suicidal, distraught, or missing person. In those scenarios, there simply isn't enough time to comply with the proposed requirements that are set forth in the amendments to section 803-44.5 and section 803-44.6, H.R.S.

The Department respectfully recommends the following amendment to S.B. 2454. The Department is requesting that a fourth exception be added to the proposed legislation, as proposed below:

§803 - Cell site simulator device; collected data, prohibition, exceptions. The State or any political subdivisions shall not, by means of a cell site simulator device, collect or use a person's electronic data or metadata without:

(1) That person's informed consent;
(2) A warrant, based on probable cause, that describes with particularity the person, place, or thing to be searched and seized; or
(3) Acting in accordance with a legally recognized exception to the warrant requirements; ~~or~~
(4) **A good faith belief that an emergency involving a danger of death or serious bodily injury to any person requires the use of a cell site simulator device without delay, in which case, the government entity that collects or uses the data shall comply with the reporting requirements set forth in section 803-47.**

The proposed amendment is consistent with HRS Section 803-42(b)(11), which was enacted in 2012. Section 803-42(b)(11) is the "exigency provision" to Hawaii's wiretap, trap and trace, and pen register laws. It allows for the "emergency" intercept of communications, even content, when an emergency involving a danger of death or serious bodily injury requires that law enforcement compel a service provider to provide information without delay. Section 803-42(b)(11) does not require a court order, search warrant, or any prior judicial approval. The intent behind the existing statutes is that if a true emergency does exist, there is simply not enough time to obtain a written court order. The rational for compelling a service provider to disclose communications without a court order applies equally to emergency scenarios involving a cell site simulator.

For the foregoing reasons, the Department of the Prosecuting Attorney of the City and County of Honolulu opposes S.B. 2454 but offers suggested amendments. Thank you for the opportunity to testify on this matter.

LATE

TESTIMONY ON SB2454 Relating to Electronic Eavesdropping

Michael Greenough - 2.2.18

Aloha Chair Kim and Committee members, my name is Michael Greenough, and I am here today testifying as private citizen.

Cell tower simulators, also known as a Stingray or IMSI catchers, are invasive cell phone surveillance devices work by mimicking the legitimate cell towers used by companies like Verizon, AT&T, and Sprint. They catch the signals emitted from cellphones and other mobile devices and extract insight into who owns the phone, his or her location, and other details.

They also send out signals to trick cell phones in the area into transmitting their locations and identifying information. When used to track a suspect's cell phone, they also gather information about the phones of countless bystanders who happen to be nearby.

It's a bit like someone setting up a big blue box, posting a United States Postal Service logo on the side, copying information from the letters that the fooled users deposit in it, and then soon after going through every piece, dumping the accumulated mail into a real mail box. No one need be the wiser.

- These Stingrays are Radio-equipped computers with software that can use arcane cellular network protocols and defeat the onboard encryption. Whether your phone uses Android or iOS, it also has a second operating system that runs on a part of the phone called a baseband processor. The baseband processor functions as a communications middleman between the phone's main O.S. and the cell towers. And because chip manufacturers jealously guard details about the baseband O.S., become too challenging a target for garden-variety hackers.

- Full-featured devices such as the VME Dominator, not only capture calls and texts, but even actively control the phone, sending out spoof texts.

- A handful of states, including Virginia, California, Minnesota, and Utah have similar laws on the books. Washington's, though (which this bill is modeled after) imposes extra requirements that compel police to describe the technology and its impact in detail to judges—presumably despite any nondisclosure agreement that those agencies may have with the FBI and the dominant manufacturer of the devices, Harris Corporation. Both the FBI and Harris have previously refused to respond to direct questions concerning the existence and use of these devices.

- The secretive surveillance devices are not only used to determine a phone's location, but they can also intercept calls and text messages. During the act of locating a phone, stingrays also sweep up information about nearby phones, not just the target phone.

Stingrays typically spoof a cell tower and force phones to connect to it, often by making the handset step down to 2G, which does not require encryption.

- Worse still, prosecutors nationwide from St. Louis to Baltimore seem to be more interested in dropping criminal charges rather than having to reveal details of stingray use.

- The ACLU has so far identified 72 agencies in 24 states and the District of Columbia that own stingrays, but because many agencies continue to shroud their purchase and use of stingrays in secrecy, those numbers are thought to drastically underrepresent the actual use of stingrays by law enforcement agencies nationwide.

The Washington law was prompted by revelations about police use of stingrays in Tacoma without warrants and without informing judges. The new law has unique language requiring that not only must a probable cause-driven warrant be obtained before a stingray can be deployed but that law enforcement must explain in detail to the judge what exactly is being done. Significant is the language requiring full disclosure to the judge of details about how and where the stingray will be used, and its capabilities and expected effect on bystanders. ...

The Washington bill was introduced just five months after Kate Martin at the Tacoma News Tribune broke the story that not only were Tacoma authorities using stingrays, but local judges did not fully understand the technology.–

"If they use it wisely and within limits, that's one thing," Ronald Culpepper, the presiding judge of Pierce County Superior Court, told the newspaper in August 2014. "I would certainly personally have some concerns about just sweeping up information from non-involved and innocent parties—and to do it with a whole neighborhood? That's concerning."

Judges like Culpepper were likely signing off on the use of stingrays not based on a warrant application but on a pen register and trap and trace order, a lower legal standard.

In the pre-cellphone era, a "pen/trap order" allowed law enforcement to obtain someone's call metadata in near real-time from the telephone company. Now, that same data can also be gathered directly by the cops themselves through the use of a stingray. In some cases, police have gone to judges asking for such a device or have falsely claimed a confidential informant but in fact have deployed this particularly sweeping and invasive surveillance tool.

Most judges are likely to sign off on a pen register application, not fully understanding that police are actually seeking permission to use a stingray. Under both Washington state law and federal law, pen registers are granted under a very low standard: authorities must simply show that the information obtained from the pen register is "relevant to an ongoing criminal investigation"—a far lower standard than being forced to show probable cause for a search warrant or wiretap order.

A wiretap requires law enforcement to not only specifically describe the alleged crimes but also to demonstrate that all other means of investigation had been exhausted or would fail if they were attempted. In the wake of the Tacoma News Tribune's reporting on stingray use in Tacoma, in November 2014, judges there imposed stricter standards.

The American Civil Liberties Union (ACLU), which has long supported more stringent standards surrounding stingrays, said that the new language is crucial.

"The language you point out in the Washington bill is significant because it aims to minimize the detrimental impact on bystanders whose phones are ensnared by a stingray," Nathan Wessler, an ACLU attorney, told Ars by e-mail.

"Also significant is the language requiring full disclosure to the judge of details about how and where the stingray will be used, and its capabilities and expected effect on bystanders. Only with that kind of full and accurate information can judges fulfill their constitutional duty to oversee and constrain law enforcement surveillance activities. The Washington law was prompted by revelations about police use of stingrays in Tacoma without warrants and without informing judges. As similar patterns are uncovered around the country, we expect to see similar legislation introduced elsewhere."

I thank you for your time in considering this measure.

Links

ACLU article on wh has them, includes map of states where these devices are being used, so far
https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them

US Senaros Question FBI over use of Stingrays
https://www.washingtonpost.com/news/the-switch/wp/2015/01/02/senators-question-fbis-legal-reasoning-behind-cell-tower-spoofing/?utm_term=.511bcb893ddf

Google search que
https://www.google.com/search?q=states+with+cell+tower+spoofing+laws&oq=states+with+cell+tower+spoofing+laws&aqs=chrome..69i57.9102j0j8&sourceid=chrome&ie=UTF-8