HCR 225, Twenty-first Century Privacy Law Task Force

Meeting Minutes

10:30 a.m., September 26, 2019

Hawaii State Capitol, Conference Room 229

Task Force members in attendance (5): Senator Michelle Kidani (Co-Chair); Representative Chris Lee (Co-Chair); Executive Director of the Office of Consumer Protection Stephen Levins (Designee of Director of Commerce and Consumer Affairs Catherine Awakuni Colon); Chief Information Security Officer Vincent Hoang (Designee of Chief Information Officer Douglas Murdock); and Deputy Prosecuting Attorney Chris Van Marter (Designee of Acting Prosecuting Attorney of the City and County of Honolulu).

Others in attendance: Oren Chikamoto, American Council of Life Insurers in Hawaii; George Cordero, ACLU; Danny Cup Choy, Hawaii Public Policy Advocates; Mandy Fernandes, ACLU; Danicia Honda, Senator Kidani; David Louie, Kobayashi, Sugita, and Goda, LLP (Facebook); Myoung Oh, Spectrum; Matthew Prellberg, Representative Lee; Luis Salaveria, SANHI (Microsoft); Radji Tolentino, Department of Commerce and Consumer Affairs-Office of Consumer Protection.

Agenda

A. Chairs' welcome

Representative Lee opened the meeting at 10:35am, and welcomed the Task Force members and audience.

B. Short recap of previous meeting

Representative Lee briefly went over what was discussed at the August 21, 2019 meeting. See August 21, 2019, meeting minutes for details.

C. Capitol website

Representative Lee confirmed that a webpage has been created for the Task Force on the capitol.hawaii.gov website. The address is:

http://capitol.hawaii.gov/specialcommittee.aspx?comm=tfcpltf&year=2019.

D. Discussion of twenty-first century privacy law topics facing Hawaii

a. Areas of risk identified by Task Force members

Representative Lee: We asked the Task Force members to identify which privacy risks they felt the Task Force should examine and potentially provide recommendations for. The only member who submitted risks was Deputy Prosecuting Attorney Van Marter. We have passed out the information he provided. Deputy Prosecutor, can you take us through it?

Deputy Prosecuting Attorney Van Marter: Yes. Hawaii has three statutes that cover law enforcement's access to electronic communications, sections 803-47.6, 803-47.7, and 803-47.8, Hawaii Revised

Statutes. Currently, electronic communication information is separated into three categories: (1) content (email, text messages, etc.); (2) transactional records (cell phone site data, internet protocol logs, email header information, etc.); and (3) basic (subscriber or account information). These three categories of information are assigned certain privacy protections. The greater obtrusion into privacy, the higher the burden on law enforcement to access the information. Basic is the lowest threshold, and law enforcement access only requires a subpoena. Access to transactional records requires a court order, and access to content requires a search warrant. Last year, the United States Supreme Court held that a search warrant is required in order for the government to access transactional records. Because Hawaii law is less stringent than the Supreme Court decision, my proposal is to do away with different categories, and require the government to obtain a search warrant for all electronic communications, with the only exception being if a user, subscriber, or customer consent to providing the information.

I also recommend changes to when notification of a search warrant has been issued for electronic communication must be disclosed. Cybercrimes received 175 search warrants in 2018, and in each case it asked for non-disclosure. No one got notice. The recommendation is to allow the court to have that discretion, but require we provide notice to service no later than time of criminal case. This proposal is to bring the statutes up-to-date and in line with current law enforcement practices.

Lee: Thank you. Is everyone okay if we go through everything else first and come back to this topic?

Task force members nod in agreement.

b. Areas of risk identified by public

Lee: While we did not get other thoughts from members, we did receive ideas from the public.

First was from Kelly McCanlies, who identified three main areas. In her presentation last week, Kelly summarized sixteen areas of interest, but specified three as low hanging fruit: (1) expanding the definition of personal information in HRS; (2) requiring an explicit opt-in or opt-out for consumers before their data can be sold; and (3) regulation or registration of data brokers.

We also heard from Jael Makagon, a privacy professional and attorney who works in the Santa Clara County Privacy Office in California. Jael is originally from Hawaii. His suggestions include reviewing: privacy related to information held by Internet Services Providers; the regulation of data brokers; facial recognition and surveillance technology used by government entities, and general government privacy principles.

The Hawaii branch of the Screen Actors Guild-American Federation of Television and Radio Artists union provided us information relating to deep fake technology.

And lastly, ACLU-Hawaii brought up concerns about government use of facial recognition technology, and facial recognition technology generally.

Mandy Fernandes, ACLU-Hawaii: ACLU can speak now if the chairs would like, or we are available to speak at the next meeting if the Task Force would like a more in-depth discussion of facial recognition technology.

Van Marter: I can share that the Honolulu Police Department uses facial recognition under a program operated by the Attorney General's office. The program is only used to assist in identifying a potential

suspect. For instance, if there is an image from surveillance at store, if the system works, it identifies a photo, and the photo is used in a lineup. If there are policies for the program, they would be online. If the program identifies a match, it is not probable cause.

Law enforcement will have strong objections to any attempts to ban facial recognition, as they will have to go back their system from the 1980s, which is thumbing through tall books of mugshots and trying to find a match. To my knowledge, there has been no abuse of HPD using facial recognition. We process thousands of thousands of cases, and I have not heard of any abuses. I am happy to listen to arguments about the issue. I read the article citing the ACLU study.

Lee: We will throw that on the next agenda and we will invite HPD to discuss and present. Is there anything else Task Force members would like to dive into?

Senator Kidani: I have some questions for the Deputy Prosecutor. Going over what you've proposed, you said that law enforcement does not have a court order or search warrant to get certain information. What is needed for law enforcement to access electronic communication in cases that are emergencies?

Van Marter: Chapter 803, Hawaii Revised Statutes, was revised in, I think 2012, to include an exigence provision. If there is an emergency in which there is a risk of death or serious bodily injury, law enforcement has the authority to reach out to a service provider to receive real time information, like a cell phone location. HPD has not used this authority much, but it has been used, sometimes in high profile situations. At least one time they thought there was a possible murder. Service providers have a form, in this case it was T-Mobile, which HPD fills out saying there is immediate danger, and then sends it to the provider for real time electronic information. We do not believe most scenarios presented to our office are true emergencies, and thus the statute cannot be used. Law enforcement would like to use it more, but we just follow the statute. Child kidnapping could count as an emergency. In the case I referred to before, T-Mobile provided real time cell location data for about twelve hours. It can take about thirty minutes or sooner to get the form filled out and submitted to the provider. Hawaii law requires a sworn declaration by law enforcement, which is not in federal statute. This is only used a couple times a year on Oahu.

Kidani: My concern is that should this law be used, who is called? A mainland or local office, because Hawaii is three to six hours behind the mainland.

Van Marter: We call the major provider and go through its legal compliance subpoena sections.

Kidani: Are they operated twenty-four hours?

Van Marter: Yes, and we've never had a problem contacting them. Our concern has been the police legally complying with the statute.

Executive Director Levins: Would your proposal affect the Office of Consumer Protection's ability to get account information from a carrier? Right now, if we subpoenaed the information and there is a website we thought was defrauding people, and we are seeking something from the basic category, would we require a search warrant?

Van Marter: Yes, although some prosecutors may want to use subpoenas. But after the Hawaii Supreme Court did away with the third-party doctrine, a person does have an expectation of privacy from third party providers. Our office stopped using subpoenas when seeking information. Since 2014,

we use search warrants. Last year there were 175. Statute says we can ask for an administrative subpoena to get call detail records, but I don't think our Supreme Court would agree with that.

Levins: Do you think this would extend to civil?

Van Marter: The Court did not say, so I cannot say.

Levins: I will take a look at it.

Chief Information Security Officer Hoang: Are you referring to digital takedowns?

Levins: Yeah, if someone has a website up and we want to take it down because Hawaii residents have been or are being defrauded. Sometimes we need to use out-of-state subpoenas or go through other steps.

Hoang: When we see something fraudulent, we just send out a notice and report to providers, we do not try to take it down, but they usually do.

Levins: We want to know who is responsible if people have been defrauded.

Lee: What other issues does the Task Force want to examine?

Levins: Kelly floated her definition of personal information to our office, and I thought it was fine. I agree that this definition needs change. A lot has happened in the last fifteen years since it was created.

Lee: Kelly also mentioned data brokers, and opt-in opt-out provisions. Maybe we can have discussions on these other topics and more presentations.

Levins: I think she was proposing registration for data brokers.

Lee: Yeah, that’s right.

Levins: I've always had problems with registration on a personal level, because people register and that is it. It gives the industry the chance to say they are regulated, without actually being regulated. It is not helpful. If you are aware of a bad actor, you are not aware because they have registered somewhere, but because of their conduct. Just having a regulation that says you have to register, I do not think, will do very much. It creates another bureaucracy with little concrete help. If the legislature is inclined to look at data brokers and enact legislation, just a requirement to register will not really do anything.

Lee: For each of these, we can synthesize a one-page explainer of each topic and have those interested to give presentation, then have a substantive conversation.

Kidani: One thing in mind, and I'm not sure if it is something the Task Force should take up, is to review the ability to report intrusions of privacy through email and phones. Being the Education chair, knowing that children have access to laptops. Even with the protections we have in place right now, even state email, we get lots of spam, etc.

Hoang: We are trying to make it better.

Kidani: I know, but with students, is there some place to report it? I have gotten a "Citibank" scam everyday for the past couple weeks. I worry for our young kids, and for our seniors. Do we have a place in Hawaii were people can go?

Hoang: Are you getting it to your capitol.gov email?

Kidani: No, to my personal cell phone.

Hoang: I think the Federal Trade Commission is the appropriate place to report to.

Kidani: Has there been any information released to the public about scams and how to report them?

Levins: There have been multiple press releases, but it is a moving target.

Kidani: Maybe release to the newspaper?

Levins: We have websites, brochures, etc.

Kidani: Can we get this information directly to our schools or through a different release?

Hoang: I know that disclosures have gotten more steam recently, but there have been a variety of campaigns to promote awareness to seniors and children. I expect this to grow more and more. Currently, it is a little sporadic.

Kidani: We should look into this further.

Lee: We can add that to the list.

Hoang: On the information technology side, we have been dealing with this for years. We are happy to work with Senate tech support team.

E. Public input

Lee: Are there any other issues that folks have a firm interest in moving forward on?

Kidani: Including from the audience.

Fernandes: I believe that search warrants for electronic information sounds like a good change. Do the less protective measures also have the disclosure changes?

Van Marter: I can only speak for the Prosecuting Attorneys of the City and County of Honolulu and our law enforcement, in order for HPD to use a subpoena to compel records from a provider, they have to go through one of two people in our office, one of which is me. Neither one of us will authorize a subpoena if HPD is attempting to get records from a suspect, because the Hawaii Supreme Court will find that the suspect has a reasonable expectation of privacy. Search warrants have gone up 400-500 percent. The only times we use subpoenas are to get records of a victim or witness, because a defendant cannot challenge someone else's constitutional rights. But were this proposal to pass, we would still give more protections to victims and witnesses.

Fernandes: May I ask a follow-up question?

Lee: Sure, but we are not trying to go deep just yet, we are just setting the agenda for the next meeting.

Fernandes, ACLU: Would victims and witnesses be notified of the subpoena?

Van Marter: We don't ask the court to issue the non-disclosure in these situations.

Fernandes: Could you?

Van Marter: You only get non-disclosure if there is risk of flight, tampering of evidence, witness intimidation, or risk of physical danger, but when dealing with a victim or witness, we do not have those factors, so we do not ask. We are concerned about contacting or arresting the suspect and danger.

Fernandes: Thank you.

Lee: Other thoughts?

David Louie, Facebook: From a process perspective, if we are going to go into a more substantive conversation, can we get the information or handouts in advance. My client's concern is balancing consumer privacy and the burdens placed on large and small businesses that have to comply with certain things in order to effectuate requirements. As a request, to the extent possible, can we get stuff out on the website?

Lee: The reason we did not want to dive in just yet is to make sure that everyone does have time to review. There will be an even more robust discussion once the legislature convenes. Our intent is for everyone to come to table. And the intent of the Task Force is to identify issues.

Are there other comments from the public or members?

F. Task Force membership

Lee: Also moving down the agenda, the chairs have started talking about inviting other members to the task forces. After this meeting, the chairs will get together to discuss recommendations for further invites.

Kidani: Once we make that decision, we will invite others to next meeting.

G. Next Steps

Kidani: We should talk about the expectations of meetings. We have not gotten into any substantive discussions yet. What are we looking at time wise?

Lee: Meetings in October and part of November, and then we have the month of December to write report. Two meetings over the next 6 weeks or so, to dive into meaningful discussion, and present recommendations. We probably will not have the time and capacity to come up with specific legislation. I do not imagine we will come to finality this time.

Kidani: I think we should do the second meeting two to three weeks after the first, in case we need a third in December. Whatever the Task Force comes up with, we still want you to testify, even if Task Force members disagree.

Lee: We'll send out the minutes as soon as they are completed, and windows for scheduling the next meetings.

Thank you everyone for your participation, we will be in touch.