**ALASKA STATE LEGISLATURE**
**HOUSE JUDICIARY STANDING COMMITTEE**
March 21, 2018
1:02 p.m.

**MEMBERS PRESENT**

Representative Matt Claman, Chair
Representative Jonathan Kreiss-Tomkins, Vice Chair
Representative Louise Stutes
Representative Gabrielle LeDoux
Representative David Eastman
Representative Chuck Kopp

**MEMBERS ABSENT**

Representative Lora Reinbold
Representative Charisse Millett (alternate)
Representative Tiffany Zulkosky (alternate)

**COMMITTEE CALENDAR**

HOUSE BILL NO. 328
"An Act relating to biometric information and to the collection, use, storage, and disclosure of geolocation information; and establishing an unfair trade practice under the Alaska Unfair Trade Practices and Consumer Protection Act."

- HEARD & HELD

SENATE BILL NO. 148
"An Act relating to powers of the Alaska Police Standards Council; and relating to background checks for admission to police training programs and certification as a police officer."

- HEARD & HELD

**PREVIOUS COMMITTEE ACTION**

BILL: HB 328
SHORT TITLE: BIOMETRIC/GEOLOCATION INFO/TRADE PRACTICE
SPONSOR(s): REPRESENTATIVE(s) CLAMAN

| | | |
|---|---|---|
| 02/05/18 | (H) | READ THE FIRST TIME - REFERRALS |
| 02/05/18 | (H) | JUD, L&C |
| 03/21/18 | (H) | JUD AT 1:00 PM GRUENBERG 120 |

BILL: SB 148
SHORT TITLE: BACKGROUND CHECKS FOR POLICE/TRAINING
SPONSOR(s): RULES BY REQUEST OF THE GOVERNOR

| | | |
|---|---|---|
| 01/18/18 | (S) | READ THE FIRST TIME - REFERRALS |
| 01/18/18 | (S) | STA, JUD |
| 02/08/18 | (S) | STA AT 3:30 PM BUTROVICH 205 |
| 02/08/18 | (S) | Moved SB 148 Out of Committee |
| 02/08/18 | (S) | MINUTE(STA) |
| 02/09/18 | (S) | STA RPT 3DP 2NR |
| 02/09/18 | (S) | DP: MEYER, GIESSEL, EGAN |
| 02/09/18 | (S) | NR: WILSON, COGHILL |
| 02/26/18 | (S) | JUD AT 1:30 PM BELTZ 105 (TSBldg) |
| 02/26/18 | (S) | Heard & Held |
| 02/26/18 | (S) | MINUTE(JUD) |
| 03/02/18 | (S) | JUD AT 1:30 PM BELTZ 105 (TSBldg) |
| 03/02/18 | (S) | Moved SB 148 Out of Committee |
| 03/02/18 | (S) | MINUTE(JUD) |
| 03/05/18 | (S) | JUD RPT 1DP 3NR |
| 03/05/18 | (S) | DP: COGHILL |
| 03/05/18 | (S) | NR: WIELECHOWSKI, COSTELLO, KELLY |
| 03/14/18 | (S) | TRANSMITTED TO (H) |
| 03/14/18 | (S) | VERSION: SB 148 |
| 03/15/18 | (H) | READ THE FIRST TIME - REFERRALS |
| 03/15/18 | (H) | JUD |
| 03/21/18 | (H) | JUD AT 1:00 PM GRUENBERG 120 |

**WITNESS REGISTER**

CERI GODINEZ, Staff
Representative Matt Claman
Alaska State Legislature
Juneau, Alaska
**POSITION STATEMENT:** During the hearing of HB 328, presented the legislation and sectional analysis on behalf of Representative Claman, prime sponsor.

JOSEPH JEROME, Policy Counsel
Center for Democracy and Technology
Washington D.C.
**POSITION STATEMENT:** During the hearing of HB 328, testified in support of the legislation.

MATTHEW ERICKSON, Executive Director
Digital Privacy Alliance
Chicago, Illinois

**POSITION STATEMENT:** During the hearing of HB 328, testified in support of the legislation.

PAM DICKSON, Executive Director
World Privacy Forum
Portland, Oregon
**POSITION STATEMENT:** During the hearing of HB 328, testified.

MELISSA GOLDSTEIN, Legal Fellow
America Civil Liberty Union of Alaska (ACLU Alaska)
Anchorage, Alaska
**POSITION STATEMENT:** During the hearing of HB 328, testified in support of the legislation.

MATHEW ERICKSON, Executive Director
Digital Privacy Alliance
Unknown City, Illinois
**POSITION STATEMENT:** During the hearing of HB 328, discussed online privacy legislation.

BOB GRIFFITHS, Executive Director
Alaska Police Standards Council (APSC)
Department of Public Safety
Juneau, Alaska
**POSITION STATEMENT:** During the hearing of SB 148, presented the legislation and offered a sectional analysis, by request of the governor.

**ACTION NARRATIVE**

1:02:52 PM

**CHAIR MATT CLAMAN** called the House Judiciary Standing Committee meeting to order at 1:02 p.m. Representatives Claman, Kreiss-Tomkins, Eastman, Kopp, and Stutes were present at the call to order. Representative LeDoux arrived as the meeting was in progress.

## HB 328-BIOMETRIC/GEOLOCATION INFO/TRADE PRACTICE

1:03:28 PM

CHAIR CLAMAN announced that the first order of business would be HOUSE BILL NO. 328, "An Act relating to biometric information and to the collection, use, storage, and disclosure of geolocation information; and establishing an unfair trade

practice under the Alaska Unfair Trade Practices and Consumer Protection Act."

1:03:53 PM

CERI GODINEZ, Staff, Representative Matt Claman, Alaska State Legislature, presented the legislation and sectional analysis, and read her testimony as follows:

> Locational privacy refers to the idea that we are able to pass through public spaces without our every movement being systematically and secretly recorded for later use. While locational privacy may have seemed like a given just over a decade ago, increasingly our movements are no longer private. Sheer location information, data identifying a person's whereabouts generating using digital information process through the internet is being collected and sold, frequently without our knowledge. Knowing where an individual is located often means knowing what that person is doing. This knowledge in the hands of advertisers, insurance agents, employers, friends, family, and complete strangers could have undesirable consequences for the individual. Similarly, biometric data, physical characteristics of an individual ranging from voice to fingerprints plays an increasingly central role in the way we interact with technology. It is estimated that by 2020, nearly 90 percent of businesses will use biometric authentication. It is critical that these data are used and stored in a responsible way. Unlike a password or user name, biometric data is difficult, if not impossible to change. If comprised, this information is comprised for good. Mismanaged biometric data in a commercial setting could allow discriminatory practices based on appearance or genetic makeup. Facial recognition technology could allow individuals or companies to track people in public spaces without their knowledge or consent. House Bill 328 seeks to ensure that geolocation information and biometric data are collected, disseminated, and stored in a responsible transparent way. Unregulated, geolocation information and biometric data not only threaten an individual's privacy but also threaten freedom of expression and association.

If we consider privacy to be a fundamental American right, then we need to consider updating Alaska Statute to protect individual privacy in the Twenty-First Century. To this end, Section 1 of the bill requires that before collecting an individual's biometric data, the collector notified the individual that the data is being collected, the purpose for which it is being collected, and the length of time for which it will be stored. The collector must receive the individual's consent to these terms which the individual can revoke or change at any time. It specifies the circumstances under which a collector can disclose biometric data and requires that a collector destroy biometric data that is no longer needed within 120-days. Persons found to have intentionally violated any of these requirements are liable for a $1,000 fine, except in cases where the violation resulted in profit for which the penalty is $5,000.

1:06:33 PM

Section 2 sets up similar protocol for the handling of geolocation information. Prior to collecting, using, storing, or disclosing an individual's geolocation information, the person must notify the individual that the information will be collected, and the purpose for which it will be collected, provide an easy online means for accessing the information collected, and obtain express consent to the disclosure. It includes exceptions in certain emergency situations, such as when a parent is attempting to locate a child or a person is attempting to provide emergency services. Persons found to have intentionally violated any of these requirements are liable for $1,000 or the total value of the damages incurred, whichever is greater, and any other relief the court deems appropriate.

1:07:17 PM

Section 3 amends AS 45.50.471(b) to include violation of geolocation information under the terms, unfair methods of competition and unfair or deceptive acts or practices.

Section 4 applies Section 2 of this bill to contracts entered into on or after the effective date of this Act.

Section 5 replaces the phrase "this chapter" with "AS 18.13.010-18.13.100" [wherever] it appears in those sections.

CHAIR CLAMAN opened invited and public testimony on HB 328.

1:08:38 PM

JOSEPH JEROME, Policy Counsel, Center for Democracy and Technology. He advised that the Center for Democracy and Technology is a non-profit, non-partisan technology advocacy organization. He explained that precise geolocation and biometric data are highly sensitive pieces of information that reveal a great deal about individuals. Yet, for most Americans, there are limited restrictions on when this information is collected and how it can be used. He described that precise geolocation data takes just two points of data, when using an app at a coffee shop and then at a grocery store, to identify more than 50 percent of folks. In the event there are more data points, it becomes much easier to identify folks. Location data reveals various information that people might not want shared, including where the person lives, travels, works, and/or prays. This information is highly sought after by industry because it allows it to build incredibly detailed profiles about individuals and, he pointed out, the industry is aware that many people are hesitant to share this type of sensitive information. Through trade associations, "companies have spent millions of dollars lobbying in any kind of regulation of privacy," including the simple requirement to ask people for permission before they use their location information. He noted that everything from flashlight applications to dating services now traffic in location data. Executives of companies that range from Ford Motor Company to Movie Pass have talked up their ability to track users without their knowledge. He described that it is reasonable to require permission from individuals and an important manner in which to create more transparency about who is collecting and using this information. Oftentimes, people tend to believe that their devices offer settings to control the sharing of location information, which is accurate, except companies do not simply rely on phone GPS information to confirm a person's location. Advertising networks and mobile location analytics companies have repeatedly gone around location controls, (indisc.) location by snipping information

from WiFi networks which must necessarily broadcast information to let users connect, but they also basically end up creating a digital map of our world.

1:11:17 PM

MR. JERONE explained that the other component of this bill is biometric data, which is "who we are" and it is inherently sensitive, using intrinsically identifiable "and you just cannot change it." It is the Center for Democracy and Technology's contention that individuals need to have control over biometric data technology (BDT) systems that wish to micro-analyze "our faces" to figure out things such as, sexual orientation, race, gender, and/or mood. Rather than recognizing that people need to be given information about biometrics and given the opportunity to decide whether "that's okay," industry has repeatedly resisted any sort of common sense limits on this power.

1:12:21 PM

REPRESENTATIVE EASTMAN requested the definition of "private person" when it comes to geolocation information, and how government agencies are specifically exempted.

MR. JEROME responded that when considering HB 328, it is important to consider exactly "who you want to cover." Internally, the Center for Democracy and Technology debated whether biometric data includes individuals. He offered a scenario where, under this bill, perhaps neighbors could sue neighbors because they were deploying certain technologies at a neighborhood gathering, or Thanksgiving, so it is important to scope exactly who the legislature wants covered under the bill. In the event the committee was concerned about commercial uses of these technologies, he pointed to the lack of transparency which can impact, in some respects, how government can sometimes obtain access to biometrics and location technologies. In general, he explained, these technologies are developed by private companies and vendors who offer their services to commercial stores and governmental departments alike. He contended that there is a tremendous lack of transparency into who these vendors are, what sort of protections they put around this data, and to whom they are offering this technology. These points, he offered, are absolutely worth debating when considering HB 328, and expressed that the states are the true innovators on privacy protections. The industry will say that these privacy issues can be enforced by the United States

Federal Trade Commission, except the United States Federal Trade Commission is limited in its ability to police privacy and it relies on the policies that companies put in place. Many times, he said, those policies are put into place due to state law.

1:15:12 PM

REPRESENTATIVE STUTES asked whether this biometric information is the same information that was breached on Facebook when it was discovered that these biometric companies had access to people's information and were selling it.

MR. JEROME responded that if Representative Stutes was discussing the recent events regarding Facebook and Cambridge Analytica, he did not believe that would be captured under this bill's definition of biometric. In response to Chair Claman, he explained that the impact of what is going on currently with Facebook does not involve biometric information.

1:16:13 PM

MATTHEW ERICKSON, Executive Director, Digital Privacy Alliance, advised that the Digital Privacy Alliance includes technology companies, technologists, attorneys, and academics who recognize a need for better online consumer privacy. Additionally, he said, he is the director of Client Services at SpiderOak a secure cloud services technology company that has been operating since 2006. He related that HB 328 is essentially guarding Alaskans' privacy and seeks to protect two extremely sensitive categories of data, such as biometric data and geolocation information. Currently, society makes use of geolocation information everywhere, everything from weather forecasts to maps. Unfortunately, he pointed out, society has been turning a blind eye to the negative impacts of the rampant unregulated data collection that came with this technology for far too long. Currently, he explained, corporations collect and sell increasingly sensitive information about our lives without our knowledge or consent, and data breaches occur on a seemingly daily basis with the unencumbered collection and use of personal information. Specifically, he pointed out, location information poses a serious privacy and physical safety threat and headlines involving the tens of millions of people exposed every day are becoming so common place that society is almost numb to the exposures. For example, the recent revelations involving Facebook and Cambridge Analytica wherein Facebook allowed sensitive and deeply personal information to be collected from over 50 million people without their knowledge or consent. He

contended that this is just one example of increasingly large amounts of data collection on Alaskans and Americans, and these dangers are threats to both privacy and safety. He related that this past July, the FBI warned parents that children are extremely susceptible to the dangers of the collection of personal information and that such collection poses threats to both their privacy and physical safety. The National Network to End Domestic Violence (NNEDV) warned that stalkers are increasingly utilizing technology to stalk people prior to, during, and after committing sexual violence. In 2014, National Public Radio (NPR) conducted a survey of 70 shelters across the nation and found that 85 percent of the shelters housed victims whose abusers had tracked them using GPS technology. These dangers are real, he stressed. Unfortunately, there is a gap in federal and state laws that makes tracking a person easier. Under federal and Alaska law, he advised, it is illegal for one person to stalk another; however, there are no statutes at the federal or Alaska state level clearly prohibiting a company from making and selling an app that allows someone else to secretly [obtain this information.] Trust is good for business and people are choosing to withdraw from the digital economy, he offered.

1:20:10 PM

PAM DICKSON, Executive Director, World Privacy Forum, noted that consent is prominent in HB 328, where consent would allow patients the opportunity to offer consent before being required, potentially, to give biometrics in a healthcare setting, which is unfortunately spreading throughout other states and it is chilling on healthcare. This legislation would give people the right to consent in the employment context, which is extremely important for victims of crime, members of law enforcement, the judiciary, and victims of domestic violence. It also gives students the right to consent to the collection of biometric information, including "voc tech" types of situations. She added that for any multi-national corporation in the United States, as of late May, they will be required to obtain consent under the new European privacy law, [General Data Protection Regulation (GDPR)]. The idea of consent for biometrics is one that has definitely already been legislated in most other countries and it has become a best and well-known best practice. Ms. Dickson advised that the manner in which the bill discusses purpose specification is moderate, reasonable, entirely defensible, and well written. She related that "no sale" is an extremely important aspect of the legislation, and she has spent over 25 years working on (indisc.) data broker issues. She

explained when information can be taken from a person's retail purchases all the way to their health data, and it is sold to data brokers and then used to create all sorts of mischief and unpleasantness. This legislation would stop that from happening in areas of biometrics, of which is forthcoming and already taking place, she offered. This legislation also allows individuals to litigate when there is a breach and their biometric data is illegally sold on the dark web. She referred to vulnerable populations and noted that the World Privacy Forum works with victims of crime, victims of domestic violence and stalking, law enforcement, and the judiciary because all of these individuals have significant safety and privacy considerations. These, she explained, are the people who benefit immediately and profoundly from the requirement for consent because they will not have their identification and authentication information simply grabbed from them without their knowledge or consent. This type of biometric data can be cross-walked to full identity information and that is where the real risk is located, she stressed.

1:24:22 PM

MELISSA GOLDSTEIN, Legal Fellow, America Civil Liberty Union of Alaska (ACLU Alaska), noted that privacy is an essential Alaskan value and that the American Civil Liberty Union of Alaska (ACLU Alaska) supports HB 328 because it protects Alaskans' geolocation and biometric information. Private companies can use private information which specifically affects Alaskans. She reminded the committee that earlier today it learned that Google can track a person's geolocational data, thereby, putting together a timeline map of everywhere a person has been as long as they have Google on their phone. She referred to Facebook's Deep Space Initiative, what it means to share biometric information, and advised that Facebook collects data of individuals in photographs who do not even have a Facebook accounts as long as one of the person's friends has a Facebook account and uploads a photo of the person, thereby, giving Facebook access to the person's facial information. She pointed out that it is biometric data that cannot be changed. Facebook has photos of over two billion monthly users and all of a user's friends and their photos, and according to an engineer of the Facebook Deep Space project, this is a system that could recognize the entire population on earth. She stressed that without regulations in place, these corporations can do whatever they like with this data without advising its users. This activity could include selling this private data to third parties at a significant profit and with unknown consequences.

Industry groups like (indisc.), which is heavily funded by Facebook, are trying to (indisc.) bills like HB 328, and she urged the committee to support this legislation to protect Alaskans, so they know where their data is going and consent to how their data is used.

1:27:09 PM

CHAIR CLAMAN referred to Ms. Goldstein's testimony that Google can timeline every place a person has traveled and asked whether the Google Maps app must be on, or whether it is simply the fact that the person has a Google mail account.

MS. GOLDSTEIN answered that it depends. In the event the location services are turned on, even if it simply an email app on your phone that is never sign out, if a person allowed Google to track their location, the map will populate. She then offered Google cite as follows: Google.com/maps/timeline?PB.

CHAIR CLAMAN surmised that if he had turned off the location services, he could not be followed so easily.

MS. GOLDSTEIN responded that if these location services are turned off, Google will not be able to put that map together.

1:28:25 PM

CHAIR CLAMAN, after ascertaining no one wished to testify, closed public and invited testimony on HB 328.

1:28:44 PM

REPRESENTATIVE LEDOUX requested a description of biometric information.

REPRESENTATIVE KOPP advised that the description is located under Sec. 18.13.290(1)and (2), page 3 line 31, and page 4, lines 1-4, which read as follows:

> (1) "biometric data" means fingerprints, handprints, voices, iris images, retinal images, vein scans, hand geometry, finger geometry, or other physical characteristics of an individual;
>
> (2) "biometric information" means biometric data used in a biometric system;

MR. JEROME answered that the Center for Democracy and Technology provided a detailed letter with a suggestion as to how the committee might want to define biometrics. He explained that there is not a universal definition of biometrics because it can cover anything that tries to capture physical, physiological, or behavioral characteristics. He described the definition in the bill as "pretty good," and recommended that the bill specifically include references along the lines of facial recognition or facial colorimetry under the notion of "other physical characteristics." In general, he said, other approaches to biometric legislation tends to create a giant list of potential biometrics and technologies that could be captured.

CHAIR CLAMAN referred to the 3/21/18 letter from Joseph Jerome of the Center for Democracy & Technology [contained within the committee packets] and pointed to the fairly long discussion of both biometric data and geolocation information. He commented that some of which is a critique of HB 328 suggesting that the committee may wish to change some of its language.

1:30:31 PM

REPRESENTATIVE LEDOUX asked that if this bill were to pass, how would it change the information or the practices of Google and Facebook, and exactly how would it be implemented.

1:31:33 PM

MATHEW ERICKSON, Executive Director, Digital Privacy Alliance, answered that he lives in Illinois where the 2008 Illinois Biometric Information Privacy Act (BIPA) was signed into law. Generally speaking, he advised, there is not much difference when compared to everywhere else. He explained that when there are apps that need to store a person's biometric information, the app presents what it is doing with the person's information and what to expect. For example, he said, the recent Google project to compare a person's photos with various pieces of art from major museums around the world displayed this sort of disclaimer (indisc.) "for us." He related that, generally, that is all that is necessary to comply.

1:32:29 PM

REPRESENTATIVE LEDOUX asked that if it is not noticeable, whether it would be, "if you want to use this, sign here, and everybody signs here. Or, you know, clicks to the agree because

you don't have any choice if you are going to use the Google app, or you are going to use Facebook, or whatever it is?"

MR. ERICKSON offered that a location information pop-up might be expected to come from Google Maps. For example, a person had an app on their phone targeted at a small child [and a game], the app advised that it would receive detailed geolocation information for a game that it had no purpose within which to collect that information, a person might want to think twice about it at that point.

CHAIR CLAMAN surmised that as to a game, it is not necessary to collect [location] information.

MR. ERICKSON said "Exactly." He advised that last year, the Digital Privacy Alliance performed research on a game targeted at small children, around the ages of four to five years that was collecting and sending detailed, down to the inch, GPS tracking data to three different advertising (indisc.) points.

1:33:55 PM

CHAIR CLAMAN inquired about the remedy, wherein if this bill became law, would this legislation prevent those actions from taking place or would it just give remedies if it was discovered that the collecting took place without permission.

MR. ERICKSON responded that there are remedies if the collection of location took place without permission. In the event someone wanted to stay within the bounds of the law, they would have to display this notice to the people loading on the game. For example, a parent loading their child's game for the first time might see this display and have some questions and explore the use of their child's precise location data before letting their child "run wild with the game."

1:34:41 PM

REPRESENTATIVE LEDOUX surmised that if the location data was turned on, "the powers that be in Google," would know every step a person took.

MR. ERICKSON responded that Representative LeDoux was correct, and currently they are allowed to sell it to whoever they please without a person's knowledge or consent.
REPRESENTATIVE LEDOUX mused, "And the legislature sweated real ID."

1:35:16 PM

REPRESENTATIVE EASTMAN related a scenario where an employer decided to institute some type of biometric security at the workplace. He inquired as to the rights of an employee to not participate in that type of collection of biometric data, and how the 2008 Illinois law would handle that situation.

MR. ERICKSON replied that currently security systems, for example, can use biometric information, and in this case to "just get consent," but Mr. Jerome could better speak to the exemptions in this bill. He offered that exemptions in the bill are for the use of security services, and that geolocation and biometrics are "used all over in secure settings. Just get consent."

1:36:31 PM

CHAIR CLAMAN clarified Representative Eastman's question and offered a scenario wherein, as a condition of employment, an employer wants an employee's geolocation information on the phone, and the phone is part of the job. Except, he continued, the person does not want the employer to know their location when they are not on the job. He requested a description of the employee's ability to advise their employer that they do not want to participate in that level of watching their movements when they are not working, and whether this bill or the State of Illinois law affects that scenario.

MR. ERICKSON responded that he had not heard anything on the biometric side in Illinois. Generally speaking, he commented, if a phone is provided by the employer and the employee is not on the clock, they should simply turn off the phone. He opined that this bill would not impact employment as described.

1:37:28 PM

REPRESENTATIVE EASTMAN offered a scenario wherein an employer requested retinal scans or DNA and the employee did not want to give his employer the retinal scan or DNA, can the employer require that the employee provide those samples. Under this bill, would the employee be given an opt-out and continue employment but not participate in disclosing that information, he asked.

MR. ERICKSON answered that adding opt-out language for forced disclosure is something all parties would be interested in discussing.

1:38:18 PM

MR. JEROME answered that these questions are not addressed in the current draft and are valid and important questions. Ms. Dixon mentioned that a European Data Protection Regulation is going into effect in May, and that piece of legislation broadly highlights the power and balance that exists between employers and employees. The Center for Democracy and Technology's goal, in general, is to have employers provide information as to how they will use their employees' biometric and other types of information, he said. He advised that the matter of actually protecting privacy, giving employees more affirmative rights, and creating an ability for employees to not actually say "No," is definitely something that is worthy of discussion.

1:39:32 PM

REPRESENTATIVE LEDOUX requested information as to the interrelationship between this bill, which is trying to go about things on a state-by-state basis, and the Interstate Commerce Clause.

CHAIR CLAMAN said that the committee would address that question during the next hearing of the bill.

REPRESENTATIVE EASTMAN noted that his question to take up during the next hearing is that government and specific law enforcement is exempted, except law enforcement receives most of its location data from private parties. He asked the effect this bill would have on the ability of law enforcement to ever gain access to geolocation information.

[HB 328 was held over.]

## SB 148-BACKGROUND CHECKS FOR POLICE/TRAINING

1:40:37 PM

CHAIR CLAMAN announced that the final order of business would be SENATE BILL NO. 148, "An Act relating to powers of the Alaska Police Standards Council; and relating to background checks for admission to police training programs and certification as a police officer."

1:41:23 PM

BOB GRIFFITHS, Executive Director, Alaska Police Standards Council (APSC), Department of Public Safety, advised that the Police Standards Council (APSC) was established by the 1972 legislature to establish standards for the training and hiring of police officers. Subsequent to the enactment of the original bill, corrections officers, probation officers, and municipal corrections officers were added. Since first establishing regulations in the 1970s, fingerprint-based background checks are required for police officers in the State of Alaska. He explained that two types of police officers are certified in the state, as follows: urban officers, normally referred to as police officers; and with a slightly lower set of standards the council certifies village police officers for populations under 1,000 residents and communities that are off of the road system. Oftentimes, he explained, these communities have quite a bit of limitation as far as their resources are concerned. This bill specifically targets a problem that arose approximately two years ago, and the Alaska Police Standards Council first learned of the problem one year ago. He related that the federal government changed the definition of Police Standards Councils, and rather than calling these councils part of the public safety system, "they called us a licensing agency," meaning the nationwide councils are occupational licensing boards. He explained that that change moved the council out of the realm of being able to run fingerprint-based background checks itself. The Alaska Police Standards Council had always performed the fingerprint-based background check for small communities, and two years ago it lost that ability. He explained that the council would receive the criminal histories to make certain the people were not disqualified by the standards, they were then enrolled in training and then certified as officers. This bill is specifically targeted, he explained, to allow the Alaska Police Standards Council the ability to continue to perform the fingerprint-based background checks.

1:43:49 PM

MR. GRIFFITHS advised that SB 148, Section 1 adds the Alaska Police Standards Council (APSC) to the list of all of the other agencies in the state that perform fingerprint-based background checks for occupational licenses, such as real estate agents, lawyers, and so forth. Section 1 amends AS 12.62.400(a).

MR. GRIFFITHS advised that Section 2 (indisc.) to give them the (indisc.), which he said is fairly simple. Section 3 amends the training section to include the requirement of obtaining fingerprint-based background checks before being admitted to a police occupational basic training program. Section 4 amends the APSC standards to reflect the subsequent section in Section 5. Section 5 amends the standards to add a new subsection limiting the issuance of a certificate to only people who have had their fingerprint-based background check performed. Section 6 amends the definitions of "our section" to bring it into compliance with the rest of the statute. Section 7 specifies the applicability of the Act specifically to people applying for admittance to a police training program or who are appointed as a police officer on or after the effective date of the Act. Section 8 is a notice to the statutory revisors of the change in the APSC's classification language.

1:45:51 PM

REPRESENTATIVE KOPP surmised that that this legislation simply gives the Alaska Police Standards Council the authority, again, to do what it was previously performing in order to ensure that a person applying to a police training program meets the statutory background check standards in Title 18.

MR. GRIFFITHS agreed, and he clarified that the standards are in regulation, which was part of the issue wherein the federal government requires that the standards are in statute before it will recognize it as a legitimate exemption to the federal laws.

1:46:47 PM

CHAIR CLAMAN opened public testimony on SB 148. After ascertaining no one wished to testify, he closed public testimony on SB 148.

[SB 148 was held over.]

1:48:56 PM

**ADJOURNMENT**

There being no further business before the committee, the House Judiciary Standing Committee meeting was adjourned at 1:49 p.m.