ALASKA STATE LEGISLATURE
HOUSE LABOR AND COMMERCE STANDING COMMITTEE
May 1, 2017
3:17 p.m.

MEMBERS PRESENT

Representative Sam Kito, Chair
Representative Adam Wool, Vice Chair
Representative Andy Josephson
Representative Louise Stutes
Representative Chris Birch
Representative Gary Knopp
Representative Colleen Sullivan-Leonard

MEMBERS ABSENT

Representative Mike Chenault (alternate)
Representative Bryce Edgmon (alternate)

COMMITTEE CALENDAR

HOUSE BILL NO. 230
"An Act relating to the collection of customer information by telecommunications and Internet service providers; and establishing an unfair trade practice under the Alaska Unfair Trade Practices and Consumer Protection Act."

- HEARD & HELD

PREVIOUS COMMITTEE ACTION

BILL: HB 230
SHORT TITLE: TELECOMMUNICATIONS & INTERNET PRIVACY
SPONSOR(s): REPRESENTATIVE(s) DRUMMOND

04/15/17	(H)	READ THE FIRST TIME - REFERRALS
04/15/17	(H)	L&C, JUD
05/01/17	(H)	L&C AT 3:15 PM BARNES 124

WITNESS REGISTER

REPRESENTATIVE HARRIET DRUMMOND
Alaska State Legislature
Juneau, Alaska
POSITION STATEMENT: As the prime sponsor introduced HB 230.

PATRICK FITZGERALD, Staff
Representative Harriet Drummond
Alaska State Legislature
Juneau, Alaska
POSITION STATEMENT: On behalf of Representative Drummond, prime sponsor, provided further introduction of HB 230.

CHRISTINE O'CONNOR, Executive Director
Alaska Telephone Association
Wasilla, Alaska
POSITION STATEMENT: Testified in opposition to HB 230.

ACTION NARRATIVE

3:17:56 PM

CHAIR SAM KITO called the House Labor and Commerce Standing Committee meeting to order at 3:17 p.m. Representatives Kito, Birch, Knopp, Sullivan-Leonard, Stutes, and Josephson were present at the call to order. Representative Wool arrived as the meeting was in progress.

HB 230-TELECOMMUNICATIONS & INTERNET PRIVACY

3:18:45 PM

CHAIR KITO announced that the only order of business would be HOUSE BILL 230, "An Act relating to the collection of customer information by telecommunications and Internet service providers; and establishing an unfair trade practice under the Alaska Unfair Trade Practices and Consumer Protection Act."

3:19:37 PM

REPRESENTATIVE HARRIET DRUMMOND, Alaska State Legislature, as the prime sponsor introduced HB 230. She spoke as follows:

> House Bill 230 is legislation aimed at maintaining Alaskans' Internet privacy. House Bill 230 is designed to keep any telecommunications service or Internet service provider from collecting personal information of a private customer without the consent of the customer in order to protect the privacy and individual liberty of every Alaskan. Alaska is one of the most independent states in the union, which is reflected by the citizens who live here. As

technology continues to change rapidly, HB 230 is needed to protect our constitutional right to privacy. House Bill 230 will protect the privacy of Alaskans' personal information stored on a cyber-based utility. I believe this bill is the best way to start addressing Internet privacy concerns. My office has received a lot of calls and e-mails from people concerned with the privacy rollbacks enacted at the federal level recently and this is an area where we cannot afford to take a wait-and-see approach. Technology moves much faster than legislation and so I want to thank you again for taking this bill up this late in the session.

3:21:16 PM

PATRICK FITZGERALD, Staff, Representative Harriet Drummond, Alaska State Legislature, on behalf of Representative Drummond, prime sponsor, provided further introduction of HB 230. He noted that cell phones, computers, laptops, and tablets are modern tools used by private citizens to conduct commerce and trading. Online shopping and bill paying are popular and provide easy accessibility to businesses. He continued as follows:

Many of these devices have the capability to retain memory, on any account number, Social Security number, credit card information, medical information, and online purchases, just to list a few. Passing of HB 230 would put into law that telecommunications companies and Internet service providers must be given consent by the user of the service or device before collecting, selling, trading, or gifting information entered by a private citizen. [House Bill} prevents discrimination of any user who declines to allow the sharing of personal information by the telecommunications companies and Internet service providers. House Bill 230 simply restricts large companies from selling information of private citizens to the highest bidder without the consent of the user. Passing HB 230 will assure users of cyber-connected devices that no information is collected without the express written consent of the user. House Bill 230 keeps Alaskan information private, preserving the privacy and independence of every Alaskan.

3:22:42 PM

REPRESENTATIVE STUTES asked whether telecommunications companies in other states are collecting, selling, or distributing this information.

MR. FITZGERALD replied that he participated in a teleconference with states that are also pushing this legislation through their state legislatures and was told that 12 other states had similar legislation. States on the call included Maryland, Hawaii, Montana, Washington, Connecticut, Pennsylvania, and Alaska, he related. There is fear of large companies like Comcast and CenturyLink. He said he has talked to representatives from local telecommunications and Internet service providers (ISPs) in Alaska who said they do not sell or distribute private information. This bill, he stressed, is not in any way an accusation that they do that or might do that. The bill just puts in protection that people will be aware of opting in or opting out of the distribution of their information.

REPRESENTATIVE STUTES offered her understanding that HB 230 is an action as opposed to a reaction.

MR. FITZGERALD responded, "Yes."

3:24:15 PM

REPRESENTATIVE BIRCH stated he is encouraged to learn that it is not a response to a problem. He said he has a fact sheet that says it is already illegal to sell or share consumer personal or sensitive information. He therefore asked what the bill is trying to accomplish if it is not responding to a situation of information being compromised.

MR. FITZGERALD answered that all the legality concepts or terms are on the federal level; Alaska has no statutes that protect Alaskans from any sort of information collecting or sharing. The sponsor, he explained, is putting in the bill [to create] a state mandate so anything that happens on the federal level doesn't result in Alaska having to react to something. It would be a state level of protection.

REPRESENTATIVE BIRCH offered his understanding that if something were illegal at the federal level it would also be illegal at the state level.

MR. FITZGERALD replied that many of the states participating in the teleconference made it clear that with the rollback of the

previous presidential administration's Federal Communications Commission (FCC) regulation, they were concerned about more FCC regulations changing. The common thread in these bills, he said, is a prevention of anything that would change on the federal level to protect the citizens of the states.

3:26:22 PM

REPRESENTATIVE KNOPP noted that for every computer application or program there are terms of use that require [the user to] check a box in agreement, which has been done since invention of the Internet, so it is widely done. He further noted that global positioning systems (GPS) on cell phones track everything. He said he is therefore trying to figure out whom this is going to apply to and what they are going to have to do. He requested further details on the bill and asked who is not notifying customers about data collection.

MR. FITZGERALD responded that essentially HB 230 would create an opt-in/opt-out concept for the data sharing. Essentially the practice of it would be another box that someone would check to say that the company does not have permission to share any of the user's personal information.

3:28:27 PM

REPRESENTATIVE SULLIVAN-LEONARD, regarding what is prompting HB 230, inquired whether something has happened within the telecommunications world where information has been sold. She related that according to all the information she has received thus far, FCC and Federal Trade Commission (FTC) regulations are being followed.

MR. FITZGERALD answered that it is just a state barrier if anything were to change on the federal level that would allow companies to sell or share information of private individuals. The bill would already protect all Alaskans from having that happen to them.

REPRESENTATIVE SULLIVAN-LEONARD asked whether at this point in time the sponsor has a record of anything being sold through the telecommunications systems.

MR. FITZGERALD replied no and clarified that this is not at all an "us versus the telecommunications companies deal." He said it is just trying to protect the private citizens of Alaska from having their information shared.

3:29:47 PM

REPRESENTATIVE JOSEPHSON inquired about what information is being referred to. For example, he said, he ordered the size 44 long sports coat that he is wearing, and it was delivered down the hall to suite 102. He inquired whether it is a matter of not wanting other companies to know he wears a 44-long coat or a matter of not wanting others to know he is in suite 102.

MR. FITZGERALD responded that personal information is not defined in the bill currently; it is just personal information in general. According to Legislative Legal and Research Services, he related, if there is no specific definition in the bill then the definition in the dictionary is what would be referred to. He said the sponsor is open to receiving a friendly committee substitute (CS) that uses the definition found in AS 40.25.350, which states:

> "personal information" means information that could be used to identify a person and from which judgments can be made about a person's character, habits, avocations, finances, occupation, general reputation, credit, health, or other personal characteristics, but does not include a person's name, address, or telephone number, if the number is published in a current telephone dictionary, or information describing a public job held by a person;

MR. FITZGERALD noted that by that definition, what is not wanted to happen, for example, is if someone should start having heart issues and by virtue of logging into sites with their computer their information is distributed and sold, and their inbox becomes the target of thousands of entities selling heart medications.

3:32:10 PM

REPRESENTATIVE BIRCH inquired whether this horse hasn't already left the barn and asked what change HB 230 would bring about. For example, he said, Google has a half-trillion-dollar business where "googling" sports coats results in numerous sports coat providers that magically zero in and show up. It seems like the disclosure part is pretty well protected at a federal level, he posited. As for the commercial aspects, including the tracking of people, he said he is convinced they know a lot about every person. He opined that HB 230 is not necessary and that

commercial enterprises are successful because they know what a person buys.

REPRESENTATIVE DRUMMOND answered that shopping on the Internet forces users to reveal a lot of personal information, credit cards being an example. She said it is not because of what happened to her and her family that she introduced this bill, but over a year ago charges showed up on her debit card bill for four nights in a Jakarta hotel. Thankfully her credit union alerted her to the charges, which occurred while she was in Juneau for a special session. Personal information is regularly being transmitted across the inter-webs, she continued, and somehow that personal information is becoming public and being used by people who do not have other people's best interests in mind. This is only part of what she is seeking to protect here, she added. Because Alaska has such specific issues mentioned in the constitution, it is incredibly important that Alaskans' privacy be first and foremost.

REPRESENTATIVE BIRCH maintained that Alaskans are currently being protected to the best extent possible. He said he isn't sure the bill is going to amp it up other than to maybe confuse the public into thinking that there is some protection out there other than what is already afforded.

MR. FITZGERALD stated the sponsor believes that HB 230 does the opposite of confusing the public; it clarifies what Internet service providers and telecommunications companies protect. With the definition of personal information, he continued, the bill is specifically saying that the person's Internet provider is protecting their information. Responding to the statement about the many markets that benefit from being able to find that information, he said he doesn't know what is or isn't protected by his Internet provider and so, if anything, HB 230 clarifies that.

3:36:49 PM

REPRESENTATIVE STUTES inquired whether anyone from the telecommunications industry would be testifying. She noted the committee packet includes letters from the industry in opposition to the bill because it would make their job so much more difficult. Given the statement that it would be a matter of checking a box to not give out a person's information, she said she is perplexed about why it would make the companies' job so much more difficult as alluded in their letters.

MR. FITZGERALD replied that the Department of Law has provided a zero fiscal note for the bill. The intent of the bill is to not make their job that much harder, he said, but to solidify that customers are being protected. From what the sponsor has heard from ISPs and telecommunications companies, they are already doing this. So, he continued, it shouldn't add any more burden to them if they are protecting the customers the way they say they are. But, he stressed, he isn't accusing them of not doing that.

REPRESENTATIVE STUTES offered her understanding that the intent with HB 230 is that there will be a question somewhere along the line [asking the company] not to give out a person's information.

MR. FITZGERALD responded that the sponsor would leave it up to the department to figure out the exact language of that. He explained it would be something along the line of, "No, I do not give permission for my information to be shared."

3:38:48 PM

REPRESENTATIVE KNOPP posed a scenario where he is on a company's website looking for a piece of equipment, and then he goes to Facebook and now ads are popping up from equipment companies. That is data collection, he said, as it is known what he was looking at and now the companies are marketing to him. He asked whether that information is coming from the Internet service providers or from the websites that he browsed, and his data is then sold to Facebook.

MR. FITZGERALD answered that according to the information he received from the teleconference, across the U.S. it is versions of both. Many people have a consensus that Facebook is a major purchaser of information, he said, and whether it is being sold by an ISP or by an individual website varies throughout the U.S. The Alaska ISPs and telecommunications companies he has talked to do not practice in that sale, he related, but the only thing keeping them from practicing that sale is their good graces. If HB 230 became law, he said, there would be state statute preventing them from doing that without the person's knowledge.

3:40:53 PM

REPRESENTATIVE WOOL, regarding data sharing, posed a scenario where he goes to a website looking for something and then afterwards everywhere else he goes has an ad for the thing he

was looking for. It is very sophisticated movement of data between all kinds of entities, he said, and he doesn't know whether there is a way to protect that shopping data from visiting various store websites. He asked whether shopping data, such as shopping for clothing, would be blocked so he wouldn't get clothing ads.

MR. FITZGERALD replied that the sponsor would rather have the department make the interpretation of what would be personal information based on the definition that was previously read to the committee, especially regarding clothes versus medical information.

3:42:41 PM

CHAIR KITO commented that it appears data is collected by Facebook as people are browsing around Facebook, by Google as people are browsing the Internet, and by Amazon as people search for items. None of those three companies are Internet service providers or telecommunications providers, but they might be the ones responsible for collecting and distributing any sort of aggregate data on purchasing history, he posited. He inquired how restricting the ability of a telecommunications provider or an Internet service provider would protect his data from being sold by Amazon, Google, or Facebook.

MR. FITZGERALD replied that it would put a restriction on the Internet service providers and telecommunications companies that operate in Alaska. Since the aforementioned companies are all headquartered outside of Alaska, it is hard for [the state] to be able to put together regulations against them. But, he continued, those restrictions should be made on a federal level and [the bill] is doing what can be done to protect the personal information with what local control is had.

CHAIR KITO asked how something like this would work with an Internet service provider or a telecommunications provider as his understanding is that they don't originate or terminate any of the data transactions; they are only the throughput component. He noted that there was a question earlier about there being federal restrictions on what those kinds of providers can do. He asked whether they are collecting the information that is going through their networks or are just passing that information through.

MR. FITZGERALD responded that the telecommunications company representatives he has talked to say they are not doing that.

However, he continued, if federal law were to allow them to do that, then that opens it up to the companies to purchase, sell, or trade any information of any private citizen in Alaska as of right now. Rather than HB 230 being a reaction to something that Alaskans are vulnerable to, the bill would implement this now, so Alaskans are protected regardless of changes on the federal level.

CHAIR KITO posited that if an Internet service provider or a telecommunications provider manages the highway, network, or series of tubes of information that go back and forth, then the packets of data are like vehicles with all the personally identifiable information inside the vehicles. The tollbooth operators are not looking inside the cars to see what is inside the cars but are just collecting the money as it goes through. He said he is therefore trying to understand what kind of personally identifiable information an ISP or telecommunications provider might have that would be of concern for public disclosure.

MR. FITZGERALD replied that most of the information is found in the definition - credit history, credit card numbers, debit card numbers, Social Security numbers, driver's license numbers. During the teleconference he attended there was a lot of talk on personal information of that sort, he related. Other states have varying degrees of what is classified as personal information and what's not. He explained that HB 230 would prevent the tollbooth of the inner web from searching vehicles. If federal regulation allowed them to search the vehicles, this bill would prevent them from doing that.

3:47:38 PM

REPRESENTATIVE BIRCH stated he has been banking online for about 10 years with a banking company that bought out a long-time Alaska bank a number of years ago. He asserted that no ISP has accessed any of that information because it is encrypted. It is more than just a vehicle on a highway, he continued, it is a package of information that basically goes from his phone or computer to his bank and he thinks that is the same with Amazon and anybody else. They can identify which website a person was in, but the ISP doesn't have access with the encryption technology. Fear is always a great motivator, he added, and he thinks it needs to be well grounded, well founded, and factual. He said he is trying to figure out how the ISP is that conduit that could tap into and access that information because otherwise the banking industry would collapse.

REPRESENTATIVE DRUMMOND responded that the Internet service provider that carried her credit card information to that hotel in Jakarta needs to acknowledge that that information is passing through its hands, its wires, its fiber, its satellite, and how her credit card information got to that hotel in Jakarta if she was physically not there and never had any contact with those people. Part of the problem, she stated, is that people are putting a lot of faith and trust in Internet service providers. She said she personally pays them a ton of money to access these services and her expectation is that they will preserve her personal information in exchange for that trust.

REPRESENTATIVE BIRCH said he is not convinced that the sponsor's ISP was the culprit in the aforementioned situation. He suggested that a person could leave behind a bank statement or there could be some other way. Most credit card companies insure their customers for that sort of problem, he noted.

MR. FITZGERALD added that HB 230 would ensure that the Internet service provider is not the culprit because of the protections that it has on personal information.

3:51:15 PM

REPRESENTATIVE KNOPP said he does understand that ISPs and telecommunications companies could collect data and that collecting and selling data is a very profitable market. He therefore doesn't discount the bill, he continued, but is just trying to understand it. He inquired whether there is any way of tracking where a breach of information occurred, such as in the case of the sponsor's credit card. He further inquired how it would be known if it were an ISP or telecommunications provider that leaked that information either erroneously or intentionally.

MR. FITZGERALD answered that HB 230 basically outlines what personal information the Internet service provider is protecting. So, if said information is let go, then hopefully the ISP would be able to at least track and notify the person that that information was leaked somehow. The bill isn't necessarily an antivirus bill or things like that, he stated, but it does prevent the Internet service provider or telecommunications company from selling, distributing, or trading a person's information.

3:53:01 PM

CHAIR KITO opened invited testimony.

3:53:16 PM

CHRISTINE O'CONNOR, Executive Director, Alaska Telephone Association, testified in opposition to HB 230. She said the Alaska Telephone Association represents telecommunications companies and Internet servers statewide. Alaska's Internet service providers are not selling private information, she stated. They are vigilant to protect customer information as well as each of the privacy policies in place, which is provided to customers when they sign up and posted on websites that define how information is collected and accessed. She related that customers are often frustrated at the additional layers of protection already required when they need to interact with association members about their accounts and private information.

MS. O'CONNOR stated that both the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) strictly regulate Internet service providers in Alaska, and that these protections are unchanged by last month's congressional action. She related that Section 222 of the [Telecommunications Act of 1996] defines how customer proprietary network information (CPNI) must be handled. She explained that CPNI is how the FCC has defined the different elements of private information and that CPNI may be summarized generally as only permitting disclosure of information as required by law, with a customer's approval, or in providing the service requested. So, there are already opt-in/opt-out provisions in place for CPNI that all association members follow. Customers receive annual disclosure notices from their providers, she continued, that explain what these rights are and that ask customers if they want to opt in or opt out of the various kinds of information.

MS. O'CONNOR pointed out that in 2015 the FCC issued guidance specifically directing providers to apply the Section 222 regulations to Internet service and these protections have not changed. In addition to the FCC, she said, the FTC has long established privacy regulations and is vigilant to identify and prosecute companies attempting to violate privacy protection.

MS. O'CONNOR stated that the Alaska Telephone Association is concerned that HB 230 proposes to add a duplicative layer of regulation and it could easily obstruct broadband service for

consumers and substantially increase provider cost. She urged that at this point HB 230 not be advanced.

3:56:21 PM

REPRESENTATIVE JOSEPHSON requested Ms. O'Connor to explain what Congress passed last month.

MS. O'CONNOR replied that Congress essentially undid the whole big net neutrality, or the open Internet proceeding, where the FCC under Chairman Wheeler had designated the Internet as regulated like an old-fashioned telephone company would be regulated. Up until that point, she explained, the Internet was under what was called light-touch regulation as opposed to traditional telecom that has many, many layers of regulation that stipulate exactly how things will be done - a lot of reporting, a lot of expensive regulation. Chairman Wheeler changed that into traditional telecom regulation, of which the framework goes back to [1934], she said. Congress set that aside and put it back to the status quo before Chairman Wheeler's order. She pointed out that it did not change the privacy regulations that [the Internet and telecom industry] have been operating under all along.

3:57:58 PM

REPRESENTATIVE BIRCH referred to the sponsor's testimony regarding loss of credit card information potentially through the fault of an Internet service provider. He requested Ms. O'Connor to describe how that credit card information could show up in Jakarta or elsewhere and have the Internet service provider at fault.

MS. O'CONNOR responded that the earlier discussion about encryption is accurate. She qualified that she is not a technical person, but she has seen recent statistics that say 50-70 percent of all Internet traffic is encrypted and all banking and all credit card numbers. The vehicles traveling on the Internet highway are actually armored cars and ISPs cannot see in them, she said, and she doesn't know a way that an ISP could have been at fault for that. She has read trade articles about black market/bad actors thieving from other retail outlets and getting thousands and thousands of credit card numbers and then stealing them. About a year and a half ago, she continued, there was a widely publicized hack of Target where the company lost hundreds of thousands of credit card numbers. So that is

one potential avenue, she added, but that is just speculation. She advised that an ISP cannot see a credit card number and she cannot conceive of a banking or other website that is not encrypted.

3:59:55 PM

REPRESENTATIVE JOSEPHSON said he is not necessarily a supporter or rejecter of HB 230. He asked whether his understanding is correct that ISPs have at the request of the federal government turned over data responsive to concerns about terrorism even though there was no law requiring it. So, he surmised, at least in that context ISPs can disclose private information.

MS. O'CONNOR answered that she is not familiar with the details of that, but she does know that through a subpoena, [information] can be requested. However, she noted, where traffic is encrypted an ISP cannot see what is there.

REPRESENTATIVE JOSEPHSON qualified he is not a scholar of this but is confident that there are ISPs which take the approach of utter vigilance and protection of privacy and there are other companies that would disclose whatever the federal government asks them to. There is this variation that the media reports, he said, and they've reported it enough that he doesn't believe it is fake news.

MS. O'CONNOR replied that her own experience from having worked for several telecom providers is that they are very conscious of following guidelines that there must be a subpoena, it must be appropriate, before any data is released. Beyond that she would have to defer to a more technical expert.

4:02:19 PM

REPRESENTATIVE WOOL offered his understanding that credit card information is not something an ISP has access to, but he asked whether an ISP has access to what websites people are shopping. He further asked whether that data that can be easily obtained, sold, transferred, or otherwise used for profit or gain.

MS. O'CONNOR responded that she believes if [information] is encrypted, it is not easily accessed, but qualified she is not an information technology (IT) expert and is willing to follow up and provide that information.

REPRESENTATIVE WOOL stated he is sure Google has access to someone's browsing history. He further surmised that ISPs or telecom companies can have good access to someone's shopping data or visits to a nefarious website. He presumed this would be something that a person with technical knowledge would be able to answer.

MS. O'CONNOR agreed that a more technical examination of this would be helpful. However, she continued, the aforementioned question raises a good point about confusion that could result with the language of HB 230. To date, it is known that Google, Facebook, and Amazon are all tracking shopping information and at what someone is looking at. Consumers do not know exactly how this is happening and one of her big concerns is that with HB 230 [ISPs and telecommunications companies] would have to prove over and over that they are not selling that ad tracking data; it is coming from the websites that the consumers are visiting.

4:04:59 PM

CHAIR KITO opened public testimony on HB 230. He left public testimony open after ascertaining that no one wished to testify at this time.

[CHAIR KITO held over HB 230.]

4:05:53 PM

ADJOURNMENT

There being no further business before the committee, the House Labor and Commerce Standing Committee meeting was adjourned at 4:06 p.m.