ALASKA STATE LEGISLATURE
HOUSE LABOR AND COMMERCE STANDING COMMITTEE
Anchorage, Alaska
December 6, 2021
1:01 p.m.

MEMBERS PRESENT

Representative Zack Fields, Co-Chair
Representative Ivy Spohnholz, Co-Chair
Representative Calvin Schrage
Representative David Nelson
Representative James Kaufman
Representative Ken McCarty

MEMBERS ABSENT

Representative Liz Snyder

COMMITTEE CALENDAR

HOUSE BILL NO. 159
"An Act establishing the Consumer Data Privacy Act; establishing data broker registration requirements; making a violation of the Consumer Data Privacy Act an unfair or deceptive trade practice; and providing for an effective date."

- HEARD & HELD

PREVIOUS COMMITTEE ACTION

BILL: HB 159
SHORT TITLE: CONSUMER DATA PRIVACY ACT
SPONSOR(s): RULES BY REQUEST OF THE GOVERNOR

03/31/21	(H)	READ THE FIRST TIME - REFERRALS
03/31/21	(H)	L&C, JUD, FIN
04/23/21	(H)	L&C AT 8:00 AM GRUENBERG 120
04/23/21	(H)	Heard & Held
04/23/21	(H)	MINUTE(L&C)
05/05/21	(H)	L&C AT 3:15 PM BARNES 124
05/05/21	(H)	Heard & Held
05/05/21	(H)	MINUTE(L&C)
05/12/21	(H)	L&C AT 3:15 PM BARNES 124
05/12/21	(H)	Heard & Held
05/12/21	(H)	MINUTE(L&C)
12/06/21	(H)	L&C AT 1:00 PM ANCH LIO DENALI Rm

WITNESS REGISTER

TRISTAN WALSH, Staff
Representative Zack Fields
Alaska State Legislature
Juneau, Alaska
POSITION STATEMENT: During the hearing on HB 159, answered questions.

MAUREEN MAHONEY, Policy Analyst
Consumer Reports
San Francisco, CA
POSITION STATEMENT: During the hearing on HB 159, answered questions.

THERESA "TERRY" BANNISTER, Legislative Council
Legislative Legal Services
Alaska State Legislature" Juneau, Alaska
POSITION STATEMENT: During the hearing on HB 159, answered questions.

ACTION NARRATIVE

1:01:20 PM

CO-CHAIR ZACK FIELDS called the House Labor and Commerce Standing Committee meeting to order at 1:01 p.m. Representatives Kaufman, Schrage, Nelson, Spohnholz, and Fields were present at the call to order. Representative McCarty arrived as the meeting was in progress.

HB 159-CONSUMER DATA PRIVACY ACT

1:02:02 PM

CO-CHAIR FIELDS announced that the only order of business would be HOUSE BILL NO. 159, "An Act establishing the Consumer Data Privacy Act; establishing data broker registration requirements; making a violation of the Consumer Data Privacy Act an unfair or deceptive trade practice; and providing for an effective date."

CO-CHAIR FIELDS noted that HB 159 is a bill offered by the administration.

1:03:14 PM

CO-CHAIR SPOHNHOLZ moved to adopt the proposed committee substitute (CS) for HB 159, Version I, as the working document. There being no objection, Version I was before the committee.

1:03:43 PM

CO-CHAIR FIELDS provided a PowerPoint presentation titled, "HB 159: The Consumer Data Privacy Act, House Labor & Commerce Committee, 12/6/2021." He displayed slide 2, "Consumer Privacy & Consumer Rights," and reminded members that the bill as introduced by the administration has four primary goals: consumers should have the right to know when businesses are collecting their personal information; the right to know what information is being collected and by whom; the right to request collected personal information be deleted; and the right to request their personal information not be sold or shared. He further reminded members that many other states have considered data privacy bills.

CO-CHAIR FIELDS showed slide 3, "Personal information: Shared, Bought and Sold," and addressed why it is timely to take up this legislation. There is overwhelming evidence, he reported, that large companies are acquiring and selling individuals' private information and are either not disclosing that or disclosing it in such a convoluted and opaque way that it effectively is not being disclosed. There are no meaningful federal standards to protect individuals' privacy, unlike in other regions and jurisdictions. Many people don't know that the information that they share, often unknowingly, online allows incredibly intimate details of their private life to be examined by many different companies with potentially profound impacts on their life, their income, and their major economic decisions.

1:05:32 PM

CO-CHAIR FIELDS moved to slide 4, "Personal Information: Shared, Bought and Sold (con't)," and continued. He stated that some of these companies that buy and sell information, often without consumers knowing their information is being bought and sold, have highly specific geolocation and biometric data, to the extent that information is highly personal and is growing with the ability of companies to collect biometric information on people. The real-world impact is on vulnerable people including youth, the potential to perpetuate systemic racism in housing lending and the acquisition of insurance, and exposure of private health care information. Also, a real risk is the abuse

of journalists and people in nonprofits doing public service who are being targeted by certain firms.

1:07:13 PM

CO-CHAIR SPOHNHOLZ realized she had incorrectly moved Version I in her earlier motion for adopting a working document. She therefore moved to adopt the proposed CS for HB 159, version 32-GH1573\B, Bannister, 11/5/21, as the working document. There being no objection, Version B was before the committee.

CO-CHAIR FIELDS requested Mr. Walsh to explain the video linked to slide 5.

1:08:08 PM

TRISTAN WALSH, Staff, Representative Zack Fields, Alaska State Legislature, addressed slide 5, "Personal Information: Shared, Bought and Sold (con't)." He pointed out the link to a video and explained that the video is from a [12/19/2019] story in The New York Times on geolocation data. He related that one transfer of geolocation data yielded 12 million phones and effectively allowed the identification of multiple people, including Department of Defense officials, politicians, journalists, and engineers.

CO-CHAIR FIELDS interjected that The New York Times was able to use publicly available information to identify where people were based on their phones. Companies are doing this, which leads a sense of urgency to legislation like this.

1:08:56 PM

CO-CHAIR FIELDS turned to slide 6, "Changes [between] Ver A and Ver B." He reminded members that the administration presented a sectional analysis during the regular legislative session. He said the purpose of today's hearing is to walk through the major changes in Version B and give members time to look through all 36 pages of the CS. He related that Version B adds protections for, and definitions of, biometric information and identifiers [Sec. 1-5]. Technology in this area and what companies are doing with people's personal information are evolving rapidly, he said, so the statute needs to be updated with respect to current practices and industry. He requested that Ms. Mahoney address best practices and legislation in other states and provide comment on the individual changes.

1:10:26 PM

MAUREEN MAHONEY, Policy Analyst, Consumer Reports, stated that as companies are expanding their collection of consumer data, including facial recognition and other biometric data, it is important that there are restrictions on what companies can do because of the chilling effects it could have on consumer privacy and consumer expression. The state of Illinois has adopted strong legislation to require consumers' consent for the collection of such data. Increasingly, states around the US are interested in pursuing similar legislation, so it is appropriate for Alaska to consider it as well.

1:11:16 PM

CO-CHAIR FIELDS returned to slide 6 and resumed his discussion of the changes between Versions A and B of the bill. He related that another change is that Version B expands the prohibition of use of consumer's data for secondary purposes beyond that which is reasonably necessary for the business for a service or activity that the consumer originally consented or requested [page 8, line 27]. He said he thinks this is a reasonable proposition. He requested Ms. Mahoney to speak to what other states are doing regarding the secondary use of data.

MS. MAHONEY stated these are important protections for consumers if you limit collection, use, and sharing of data to what is reasonably necessary to provide the service requested by the consumer. That means a consumer could use accounts and services safely without having to take any additional action, providing key protections for consumers. With Proposition 24 that goes into effect in 2023, California will have a similar protection with respect to limit use of sensitive information, but a consumer would have to take action to enable it and it is only limited to sensitive information. Alaska would be a real leader in pursuing it, she added, and it would ensure real protection for consumers.

1:13:06 PM

REPRESENTATIVE MCCARTY asked how consumers can know if their data is being used in any realm at all. He further asked whether there is a way for consumers to do a check on where their name and information is being used and who is doing that. Otherwise, he remarked, it seems very challenging.

MS. MAHONEY responded that that is one reason why prohibition on secondary use is so important. Companies are constantly collecting information about consumers as they traverse the internet and, increasingly, with offline geolocation. So, having legislation that puts the onus on businesses to only process, use, collect, and share data is necessary and can help ensure that the consumer is protected without the consumer having to take additional action because right now the consumer doesn't know what companies are doing.

1:14:35 PM

REPRESENTATIVE MCCARTY shared a story about putting out an ad for his business a long time ago. The yellow page type company wrote his name wrong for that ad, using Ken McNarty rather than McCarty. In a very quick time, every yellow page grabbed that ad, including Google and others, and it took about eight years to clean it up. He asked whether there is a mechanism in this process through which consumers can be informed about whether their information is being spread around, given that otherwise things can be happening behind the scenes.

CO-CHAIR FIELDS replied that in other countries consumers have a right to take inaccurate information off the web. He pointed out that inaccurate information can prevent someone from getting a job or a small business from succeeding.

MS. MAHONEY concurred that these are tricky issues. She stated that strong data minimization in privacy legislation would cut down on a lot of the transmission of data to third parties, whereas right now there are next to no limits on what companies can do with someone's data. She said she likes that the bill provides a right to access and a right to correction so that companies falling under it would be required to give consumers the information it collected about them and give consumers the opportunity to correct it. She concurred that, as pointed out, the horse may have already left the barn and the information may already be in the hands of many different companies. She said another thing she likes about the bill that could help make some of these protections achievable for consumers in terms of correction is that a consumer could authorize a properly accredited third party to exercise rights on their behalf. The third party could go to hundreds of companies and access the consumer's information and correct it with the consumer's permission.

1:17:49 PM

CO-CHAIR FIELDS returned to slide 6 and resumed his review of the changes made in Version B of the bill. He reminded members about their previous discussion regarding global privacy control and whether consumers have a means to opt-out of having their information bought and sold across platforms so that they are not trying to navigate what are often extremely lengthy and incomprehensible legal documents. He said Version B includes a global privacy control, a change that multiple consumer advocates recommended and that he thinks important [page 12, line 11]. It is very hard as a consumer to know how to navigate each individual application and company, he added, given that many times it is unknown by the consumer what company is being interacted with.

MS. MAHONEY reiterated that the data minimization would shut down on a lot of inappropriate data sharing in sales, but for any additional sale that is happening these browser privacy signals can make it easy for consumers to exercise their preferences to opt-out and every company with which their browser interacts online. She related that Consumer Reports was part of a group of researchers and academics and advocates to create this global privacy control, which is meant to be similar to "do not track" and to be fully compliant with new privacy laws like the California Consumer Privacy Act that requires businesses to honor a do not sell signal. She further noted that existing California regulations require businesses to honor browser privacy signals and global privacy control specifically as an opt-out of sale. Global privacy control is already in use, she added, and is a good protection for Alaskans to have.

1:20:28 PM

CO-CHAIR FIELDS returned to slide 6 and resumed his review of the changes made in Version B of the bill. He explained that another change in Version B is stronger protection for minors [including explicit requirements for protection of data of minors and teenagers with opt-in by parents/guardians for those under 13 and opt-in for those ages 13-18; page 13, lines 22-24]. He said he thinks this is appropriate to include and noted that there is a lot of competition among digital companies to capture market share of young people. Most people would consider some of those tactics as highly unethical, he added.

MS. MAHONEY agreed that children are particularly vulnerable online. She said more is being learned about how advertisements and other content that target children can be harmful.

Therefore, she added, she appreciates these extra protections for consumers, particularly around the advertisements that can be targeted to children.

1:21:56 PM

REPRESENTATIVE NELSON asked what kind of verification is given in similar laws in the US or other countries for people between the ages of 13 and 18 or under 13 years old.

MS. MAHONEY answered that she is most familiar with the California Consumer Privacy Act and the protections for children in that Act. She said her understanding of that Act is that most consumers have an opt-out on the sale of information, but for kids under 16 there are opt-in protections. Version B would be similar in that it is trying to provide more default protections for minors.

REPRESENTATIVE NELSON asked whether the opt-in for Version B would fall under a web site that directs a person to click on something [to verify] that they over age 18.

MS. MAHONEY qualified that she is not an expert on children's privacy. She offered to follow up with information.

CO-CHAIR FIELDS invited Ms. Bannister to answer the question.

1:23:55 PM

THERESA "TERRY" BANNISTER, Legislative Council, Legislative Legal Services, replied that she doesn't know whether the bill addresses how it would be determined that the person is the age they say they are. She suggested that that might need to be worked on further.

CO-CHAIR FIELDS stated that he shares interest in this question. He invited Mr. Walsh to provide an answer.

MR. WALSH responded that the bill doesn't address that specifically in the statute language, but it does authorize the attorney's general office to develop regulations for implementation of the bill. He said therefore imagines some of that could change in an ongoing basis as technology changes and that it is something the Department of Law (DOL) addresses through regulations.

CO-CHAIR FIELDS stated he would like to get something specific in this regard.

REPRESENTATIVE NELSON said he hopes something like that can be put into this legislation as it is important to have that in law and not just interpretation because children could just check that they are over 18 and get into anything they want to.

CO-CHAIR FIELDS agreed.

1:25:41 PM

REPRESENTATIVE KAUFMAN inquired about how to determine the correct cutoff age for the parental opt-in versus some other form of opt-in/opt-out. He further inquired about whether there is a legal reasoning behind it or whether there is a difference between the ages of 13 and 14 that is essential.

CO-CHAIR FIELDS referenced the concept about laws being appropriate to the brain development of minors and the ability of a minor to understand how he or she is interacting with the broader world. He noted that this is seen in criminal statutes whereby as a minor gets closer to age 18 the law assumes the minor has a greater understanding of the impact of his or her actions on other people. He allowed that what constitutes the perfect cutoff is a tough question, and requested the thoughts of Ms. Mahoney regarding whether under the age of 13, or a different age, is the right cutoff for parental opt-in.

MS. MAHONEY reiterated that children's privacy isn't her focus. She answered that a fair amount of precedent is seen, including through the California Consumer Privacy Act, for under 13 requiring parental consent, and the opt-in privacy protections for ages 13-16.

CO-CHAIR FIELDS stated that this question about age threshold can be put forth to other nonprofits which work on this privacy issue. He offered to have Mr. Walsh contact these groups.

1:28:19 PM

REPRESENTATIVE MCCARTY asked whether setting the threshold to age 14 would set a precedent as to what is a minor and what is the responsibility of parents or minors.

CO-CHAIR FIELDS replied that he doesn't think this would change the definition of minor in other areas of state statute as this

is solely in respect to data opt-in. He requested Ms. Bannister's response to the question.

MS. BANNISTER responded that this does not change any other definition in the statutes about minor and other responsibilities in the statutes. She said it merely indicates what would have to be done at certain ages, what the company would have to do and what they would need for this bill.

1:29:40 PM

CO-CHAIR FIELDS returned to slide 6 and resumed his review of the changes made in Version B of HB 159. He said a final major change is the threshold for businesses that are covered under the bill. There is much need to protect consumer privacy, he stated, but care must be taken to not burden long-standing businesses in Alaska that provide real goods and services with complex and expensive regulations to navigate when those businesses are not buying, selling, tracking, or exposing people's information in ways that most people would see as unethical. The biggest challenge of this bill is crafting a threshold that regulates those companies that are doing things that are unethical or at least should be subject to full information for consumers while protecting Alaska companies that necessarily collect consumer information but don't buy and trade it. The bill presented by the administration would have imposed sweeping regulations on a wide range of Alaska businesses, not just digital companies that are harvesting and selling people's information. The threshold in Version B, Co-Chair Fields explained, is that a company would not be regulated unless it is getting most of its income from selling this information and/or buying and selling data of 100,000 or more consumers or households. Under Version B, a large Alaska business that has information on more than 100,000 people, but isn't selling that information, won't need to hire a team of lawyers to comply with the bill. This threshold is key, he stressed, because of not wanting to burden bonafide Alaska businesses but wanting to protect consumers. He requested Ms. Mahoney to discuss some of the key choices in crafting a threshold.

1:33:47 PM

MS. MAHONEY explained that the threshold of 100,000 consumers is consistent with California, as amended by Proposition 24 in Virginia's new law, and Colorado; although, proportionately, that would be a much higher threshold for Alaska because it is pegged to the collection of data of consumers in those states.

Generally, if a company is collecting data the company should be required to adhere to privacy and security practices, but on the other hand it is important to prioritize reining in the worst actors in the state, which do happen to be the biggest companies. She said the 50 percent revenue threshold tied to data processing is appropriate and consistent with other states.

1:35:38 PM

REPRESENTATIVE KAUFMAN, regarding how that metric is applied, asked if the distinction is whether a company's revenue is coming from selling data or coming from advertisement that is enabled by the data. In other words, he continued, a scenario in which, after this bill is passed, a company could still be acquiring and using that data, but the company wouldn't be brokering the data, it would be brokering the service around it. He therefore asked whether there is an end run around this that would make it not as effective as hoped.

MS. MAHONEY answered that much of the original language for this bill was based on other states where the key protection is an opt-out sale of data, and a lot of companies have responded to that opt-out sale by saying that their data practices don't fall under the definition of sale. But, she advised, a better definition of sale is included in HB 159 than what is included in the California Consumer Protection Act that would cover a lot of monetization that doesn't necessarily cover the exchange of data. She agreed with the point that care should be taken to make sure that companies can't evade this.

REPRESENTATIVE KAUFMAN stated that information can be sold or rented by offering a utility that is informed by the same information.

CO-CHAIR FIELDS reiterated that he would have his staff reach out to experts who have followed these bills across the country and ensure that HB 159 is written as tightly as possible.

1:38:04 PM

CO-CHAIR FIELDS displayed slide 7, "Violations/Enforcement," and resumed his PowerPoint presentation. He pointed out that violations and enforcement is a key issue, and that a problem with enforcement could occur if there are no lawyers in Alaska who understand this subject matter, given the thousands of attorneys who do understand it and work for the companies that buy and sell information. In writing the CS, he explained, a

look was taken at best practices and what provisions would provide a strong enough likelihood of enforcement that it would deter illegal behavior. One key provision in Version B is that the consumer retains a right to private action. There are several attorneys who specialize in this field, so Alaskans should be able to retain those private attorneys to seek recompence from these bad actors should their information be acquired or sold illegally. The second key provision relates to building expertise at the state level so that Alaska doesn't have such an asymmetry of expertise in the fields that there is no ability to do enforcement. To ensure that the state can protect an individual's rights, Version B establishes the consumer privacy account [in the general fund] which is funded by the very companies that are buying and selling this information. The idea is that if these companies violate the law, then the state will be able to advocate for Alaskans because privacy is a constitutional right. Co-Chair Fields stressed that how enforcement is dealt with in HB 159 is a key question because if it isn't sufficiently strong, then the best language will go unenforced.

1:41:04 PM

REPRESENTATIVE NELSON posed a scenario of the bill passing in its original version without the 3 percent revenue fee. He asked whether the Department of Law would still protect Alaskans' consumer privacy.

MS. BANNISTER replied that she believes so. She said she would have to check the original bill, but under the proposed CS a violation of the new chapter would be a violation that is an unfair trade practice act, and under that there are various ways that the attorney general handles those things, such as requesting [a company] to stop doing what it is doing and by getting an injunction. Also, individuals can enforce it under the Trade Practices Act.

CO-CHAIR FIELDS confirmed that as crafted by the administration, the Department of Law would have had a role in this. However, he pointed out, DOL has no attorneys on staff who are expert in this. The state needs to prevent a situation where an outside company is violating the law, but the state has no in-house expertise to deal with it, leaving Alaskans unprotected. In crafting this CS, he explained, he wanted to be consistent with other provisions of state law. The robustness of enforcement is important to achieve compliance. Tech industry attorneys in the private sector receive very high pay and the question is how to

acquire and maintain that expertise in Alaska, so it must be robustly and sustainably funded so Alaskans are protected.

1:44:39 PM

REPRESENTATIVE NELSON opined that having this expertise in DOL would be okay if the bill is passed, but it should be going through the appropriation process, not trying to make it via a tax on the companies.

CO-CHAIR FIELDS responded that the fees would be subject to appropriation, as all are. He said he doesn't want to burden consumers with enforcing something that is a problem not created by Alaskans.

1:45:33 PM

REPRESENTATIVE MCCARTY noted that, with technology, [a company] could be anywhere in the world. He posed a scenario in which an organization is not in Alaska but is doing business quasi in the state through an app. He asked how this bill would work if the company were asked to reveal who the individuals are within the state doing business with this app, but the company refuses to cooperate, saying that it is not a business formed in the state and not responsible to the state in terms of enforcement.

CO-CHAIR FIELDS answered that the first thing a company that is illegally buying and selling Alaskans information is going to say is that an Alaska court is not a proper jurisdiction and shop around for the friendliest court in another state. If Alaska doesn't have attorneys with expertise in this, and the time to pursue it, Alaskans aren't going to get justice. The resources must be there to pursue these violations because it is correct that these companies are going to use every trick to try to evade compliance.

REPRESENTATIVE MCCARTY inquired whether Alaska has the appropriation of funds to be able to go after these entities which are located all over. Noting that there are several states doing this, he further inquired whether a compact of states could be done so that collectively there would be more enforcement ability.

1:48:49 PM

CO-CHAIR FIELDS remarked that a compact of states is a great question. He asked Ms. Mahoney whether she is aware of any states collaborating on enforcement.

MS. MAHONEY answered that she is aware of it happening on certain issues; for example, there was a big settlement with respect to credit reporting against some of the major credit reporting agencies. She said privacy is still a relatively new space with California and now Virginia and Colorado, although the laws in Virginia and Colorado are not yet in effect. She concurred that it is something to consider as more states adopt this legislation.

MR. WALSH added that there are two tracks for enforcement here. There is the state action brought by the attorney general, along with giving to the consumer the right to private action and their personal information is subject to unauthorized disclosure and sharing. He said this private action would help with compliance even if the corporation is not established in Alaska and is in another state.

1:50:32 PM

REPRESENTATIVE KAUFMAN posited that passage of this legislation would create an opportunity for an attorney, through free market incentive, to study and become an expert on the topic.

CO-CHAIR FIELDS replied that this is a unique challenge for small states, while states like California wouldn't necessarily need this. If there was a team in the Department of Law, he continued, that team would study up on the issues, violations, and enforcement actions across the country. He expressed has confidence in the people at the Department of Law for their professionalism and ability to prosecute.

1:52:40 PM

REPRESENTATIVE KAUFMAN, in regard to balancing legal need, asked whether this provision would provide a special status and thereby highlight this issue beyond other issues.

CO-CHAIR FIELDS responded that his goal is that it does not get a special status because he does not want to take away resources from prosecution of crimes of violence versus privacy rights. Given the speed at which this area is evolving technologically, along with statutes in Europe and other states, he continued, the reality is that this is a very specialized legal field. It

is more challenging to have that expertise in-state, but without that expertise the less likely it is that compliance will be achieved. He concurred that this is not more important than, say, crimes of violence, but the goal is that the Department of Law would be able to ensure compliance with this and other statutes, not prioritizing one above another.

1:54:53 PM

REPRESENTATIVE MCCARTY shared that he recently learned that the cost to be a cybersecurity expert can be $1 million per individual for their education and certifications. He asked where the co-chair sees that playing into this process of having people able to recognize infringement on people's privacy.

CO-CHAIR FIELDS answered that the state is going to spend more money bringing the expertise to protect the information of agencies and personal information of Alaskans in terms of the specialized knowledge for cybersecurity. There is corresponding specialization in the legal field and that creates a need to be thoughtful about how to have that expertise in Alaska. People in other states with this specialized knowledge earn a lot of money, whereas someone doing general cases in the Department of Law isn't going to have that specialized knowledge right now, but it is needed.

1:56:31 PM

REPRESENTATIVE MCCARTY concurred that there is the need but asked whether the cost is equal to the cost for cybersecurity. He related he has been told that the cost can be $45,000 per certification, and these certifications must be paid for by the individual and are in addition to a masters or doctorate degree. He asked whether it is being seen in other states that the standard to be acknowledged to do this work puts them at a very high level to be certified.

CO-CHAIR FIELDS replied that what a chief technology officer (CTO) would do is going to be different than what the attorneys would do to investigate and prosecute violations of privacy statutes. But, he continued, in terms of the evolution of technology and the specialization, it is analogous.

MS. MAHONEY noted that this is an emerging space. She said California is the first state to have this comprehensive privacy legislation. Its attorneys general office had to scramble to build this expertise and attract new staff, and they are under-

resourced to the task at hand. She said they were picking up this expertise on the job by tapping into experts. She added that it is important for law enforcement to have the resources needed to enforce the law and attract knowledgeable staff.

MR. WALSH recounted that in a prior hearing on the bill, experts pointed out that creation of a local privacy control might be very expensive, but that once it is an industry standard or is becoming more common, compliance itself becomes a marketing opportunity. He said there could be 50-100 transactions on the initial second or first five seconds of when a consumer clicks a website and the cookies read their visit, so compliance itself can become automated and readily accessible for many businesses.

2:00:37 PM

REPRESENTATIVE NELSON asked whether the Department of Law has been consulted on whether an attorney in cybersecurity or consumer protection is already on staff and could be trained for this expertise if HB 159 were to be passed.

CO-CHAIR FIELDS replied that he would check with DOL in this regard.

2:02:20 PM

CO-CHAIR FIELDS stated that his goal in hearing the bill today was to provide enough time for members to do research and think about potential changes prior to January. He said he would like to advance this legislation to protect Alaskans without creating onerous new regulations on Alaska businesses that are not buying and selling people's personal information.

[HB 159 was held over.]

2:03:18 PM

ADJOURNMENT

There being no further business before the committee, the House Labor and Commerce Standing Committee meeting was adjourned at 2:03 p.m.