ALASKA STATE LEGISLATURE
HOUSE JUDICIARY STANDING COMMITTEE
March 18, 2022
1:23 p.m.

MEMBERS PRESENT

Representative Matt Claman, Chair
Representative Liz Snyder, Vice Chair
Representative Harriet Drummond
Representative Jonathan Kreiss-Tomkins
Representative David Eastman

MEMBERS ABSENT

Representative Christopher Kurka
Representative Sarah Vance

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
12/06/21	(H)	Heard & Held

12/06/21	(H)	MINUTE(L&C)
01/21/22	(H)	L&C AT 3:15 PM BARNES 124
01/21/22	(H)	Heard & Held
01/21/22	(H)	MINUTE(L&C)
01/26/22	(H)	L&C AT 5:15 PM BARNES 124
01/26/22	(H)	Heard & Held
01/26/22	(H)	MINUTE(L&C)
01/28/22	(H)	L&C AT 9:00 AM BARNES 124
01/28/22	(H)	Scheduled but Not Heard
01/31/22	(H)	L&C AT 4:30 PM BARNES 124
01/31/22	(H)	-- MEETING CANCELED --
02/02/22	(H)	JUD AT 1:30 PM GRUENBERG 120
02/02/22	(H)	-- MEETING CANCELED --
02/04/22	(H)	L&C AT 9:00 AM DAVIS 106
02/04/22	(H)	Moved CSHB 159(L&C) Out of Committee
02/04/22	(H)	MINUTE(L&C)
02/04/22	(H)	JUD AT 1:30 PM GRUENBERG 120
02/04/22	(H)	-- MEETING CANCELED --
02/07/22	(H)	L&C RPT CS(L&C) NEW TITLE 1DP 4NR 1AM
02/07/22	(H)	DP: FIELDS
02/07/22	(H)	NR: SCHRAGE, SNYDER, MCCARTY, SPOHNHOLZ
02/07/22	(H)	AM: KAUFMAN
02/07/22	(H)	JUD AT 1:30 PM GRUENBERG 120
02/07/22	(H)	Heard & Held
02/07/22	(H)	MINUTE(JUD)
03/18/22	(H)	JUD AT 1:00 PM GRUENBERG 120

WITNESS REGISTER

RYAN HARKINS, Senior Director
Public Policy
Microsoft Corporation
Seattle, Washington
POSITION STATEMENT: Offered a PowerPoint presentation during the hearing on HB 159.

ACTION NARRATIVE

1:23:37 PM

CHAIR MATT CLAMAN called the House Judiciary Standing Committee meeting to order at 1:23 p.m. Representatives Snyder, Claman, and Kreiss-Tomkins (via teleconference) were present at the call to order. Representatives Drummond and Eastman arrived as the meeting was in progress.

HB 159-CONSUMER DATA PRIVACY ACT

1:24:15 PM

CHAIR CLAMAN 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."

1:24:53 PM

RYAN HARKINS, Senior Director, Public Policy, Microsoft Corporation, provided a PowerPoint, titled "HB 159 Additional Document - Microsoft PowerPoint Presentation 3.18.2022.pdf" [hard copy included in the committee packet.] He offered an overview of the history and current landscape related to privacy legislation in the United States. He referred to slide 2 of the presentation and read Microsoft's mission statement, which is to "empower every person and organization on the planet to achieve more." He said that the execution of this mission is centered around artificial intelligence (AI) technology. He added that AI technology can be any sort of automated technology, online services, or software which assists people or performs certain functions. He recommended that public policymakers regard AI as a confluence of three trends: a massive increase in processing power, new and sophisticated algorithms, and data.

MR. HARKINS noted that in the 1970s, computer scientists had created microprocessors which could process approximately 90,000 instructions per second. In comparison, current technology in smartphones can process billions of instructions per second. He explained that new and sophisticated algorithms are computer programs adept at processing large volumes of unstructured data, identifying patterns, and deriving inferences or conclusions from large sets of data. He characterized data as the most important development. He stated that people are creating, processing, storing, and using much more data than ever before. He stated that the ability to process and identify patterns from extremely large sets of data very quickly leads to much innovation. He offered examples of innovative uses of data, such as programs which perform natural language translations, spell checks, sequencing human genomes, and autonomous vehicles.

MR. HARKINS referred to the question of how rules and regulations can be created which provide protection for consumers while allowing the industry to innovate responsibly. The question is a challenge because the creation of large sets

of data and the ability to process these pose obvious difficulties regarding personal privacy.

1:30:04 PM

MR. HARKINS stated that the Microsoft Corporation has been concerned with data privacy for decades. He noted that, approximately 20 years prior, Bill Gates wrote a memo which is referred to as the "Trustworthy Computing Memo." He stated that the memo portended the rise of the commercial internet and predicted that gaining the trust of consumers would be incredibly important as more services migrated online. He added that security and privacy would be the two issues which would gain and earn consumer trust. He noted that concerns about consumer privacy have risen along with distrust in technology and in the technology industry. He stated that Microsoft's position is that legislation is necessary to provide credible privacy protections for consumers, so that trust can be earned back. He suggested that the phenomenon of distrust was not a new one. He drew attention to slide 7 of the presentation which pointed out a Harvard Law Review article from 1890 written by Samuel Warren and the future U.S. Supreme Court Justice, Louis D. Brandeis. The article addressed the right to privacy. He pointed out that the publication is the foundation for more than one hundred years of development of privacy law.

MR. HARKINS noted that the authors were responding to the development of new and invasive technologies and new business models. He revealed those technologies to be instantaneous photography and listening devices which could be used to capture personal information and make this information more broadly available. He drew a correlation to these technologies and the rise of "yellow journalism," or tabloid journalism. This led to the need for common law reform to include a tort concerning the right to privacy. He referenced the writing of William Prosser, on slide 8, which summarized the development of case law in the 70 years interceding the original article by Warren and Brandeis. He noted that the organization of this case law fell into four individual torts, which are still in existence in the United States.

MR. HARKINS noted that these developments took place before the rise of new computer technology and the internet. He noted a U.S. Department of Health and Welfare report from the 1970s which addressed the growing concerns regarding the use of computers to collect and store information about individuals, as seen on slide 9. He stated that the report had produced the

Fair Information Practice Principles (FIPPs), which govern and provide rights to individuals regarding the collection and use of their information. He noted that these principles are the basis for the Organization for Economic Cooperation and Development's (OECD's) principles, released in 1980. He added that these are the basis for the first comprehensive privacy laws passed in the European Union (EU). He stated that FIPPs had been developed first in the United States; however, no comprehensive privacy law has been passed to address privacy issues across industries and subject matters. He explained that certain narrow, industry-specific privacy laws have come into existence, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act, both pertaining to privacy in healthcare. He added that the Gramm-Leach-Bliley Act pertains to privacy in the financial sector, and the Children's Online Privacy Protection Rule (COPPA) pertains to the online collection of information on children under the age of 13. He stated that there are consumer protection laws, such as the Federal Trade Commission Act, Section 5. He also pointed out various state consumer protection laws barring unfair or deceptive trade practices. He reiterated that in the U.S. there has not been a comprehensive or omnibus approach to privacy laws.

1:37:18 PM

MR. HARKINS surmised that the lack of a comprehensive privacy law in the U.S. is in direct contrast to the 1995 EU's Data Protection Directive omnibus privacy law. He reiterated that the EU law was based on FIPPs, and it created a regulatory regime which applies to privacy issues across industries. He added that from this the General Data Protection Regulation (GDPR) was created. He noted that GDPR has become the global "gold standard" for data protection laws, with many countries adopting laws based on its fundamentals. Noting again that the U.S. does not have a comprehensive data privacy law, he stated that Microsoft has been calling on the U.S. Congress to pass such a law since 2005. He added that several states have enacted laws, the first being passed in California in 2017. He stated that the real estate developer, Alastair Mactaggart, had organized a team which drafted a ballot measure. In 2018 the ballot measure resulted in the first comprehensive data privacy law in the U.S. He added that Mr. Harkins had characterized the law as an imperfect, yet significant achievement. He continued that Microsoft was supportive of the passage of this law, and it worked behind the scenes to advance it. He said that in 2019,

in Washington State, the Washington Privacy Act (WPA) was proposed. This effort would have expanded provisions for consumer protections beyond California's law, as it had included terminology and concepts from the EU's GDPR. He stated that Microsoft has suggested that some of these concepts should be clearer and align with those in the EU, as this would aid companies doing business with EU countries.

1:42:06 PM

MR. HARKINS noted that this bill was never adopted in Washington State, though its legislature has passed similar versions of the bill. He added that a wave of proposed privacy legislation across the country has begun, pointing out that in March 2021, Virginia passed a comprehensive privacy law which was modeled on the proposed WPA. He added that Colorado also passed a privacy law which is similar to WPA. He characterized Colorado's law as stronger than the law passed in Virginia. He added that Utah has also passed a law which purports to be based on WPA; however, Microsoft has expressed concerns whether it will offer actual consumer protections.

MR. HARKINS stated that Microsoft is tracking an estimated 70 comprehensive data protection laws proposed across 30 states. He noted that Ohio, Florida, and Oklahoma, each have serious efforts to pass privacy legislation. He offered that Microsoft's standpoint is that a credible privacy law should provide for strong corporate responsibility, and it should include "affirmative obligations" on companies to responsibly steward the data they collect, regardless of whether consumers elect to exercise their right to privacy. He described an "affirmative obligation" as conducting data protection impact assessments to evaluate processing activities which analyze risks to consumers. He added that a credible privacy law should also provide consumer rights so consumers can control access to their data, with the right to delete information, correct inaccuracies, port personal data from one service provider to another, and provide consent for the activities which increase the risk of harm.

1:46:08 PM

MR. HARKINS offered that Microsoft's standpoint is that a credible privacy law should provide transparency obligations and include a strong enforcement component. He added that the challenges associated with enforcement are a significant hindrance to getting such laws passed. He posed the

consideration of whether a privacy law should include a private right of action. He stated that the laws passed in Colorado and Virginia do not provide private rights of action and include enforcement solely by the state's attorney general. He stated that the law in California has been updated by a ballot initiative passed November 2020, which provides enforcement by a data protection agency, in addition to enforcement by its attorney general. He added that California currently allows for a limited private right of action related to data breaches resulting from negligent security practices. He offered that the conversation is a difficult one and attributed this difficulty to the business community's reluctance to support a consumer's right to seek relief in court. He added that other stakeholders hold the belief that a broad, class-action liability with statutory damages should be included. He offered that the private right of action is not "all or nothing," and policymakers may consider many different elements to provide consumer protections, such as injunctive relief, attorney fees, and damages related to violations of consumer rights, in lieu of the private right of action. This would allow lawsuits in cases of "forgetting to dot the 'i' or cross the 't'" in privacy policies.

1:48:41 PM

MR. HARKINS offered that additional considerations may include whether the law would cover modern data sets, the way data is collected, and the way consumers are tracked online. He added that any credible privacy law should apply to identified data and data that is "identifiable data." He explained that "identifiable data" is data associated with a cookie, an internet protocol (IP) address, a device identifier, or another consistent identifier. He added that these types of data sets are used to track consumers online to serve consumer targeted advertising.

MR. HARKINS recommended that the term "pseudonymous data" not be used, as it is confusing and prone to abuse. He offered that the set of consumers rights in legislation should consider whether consumers are allowed to truly control their information. He offered the example of the "right to delete" and stated that the laws in California, Virginia, and Colorado each contain this provision. He explained that the law in California only applies to personal information collected from a consumer and does not apply to data collected by a third-party source, nor would it apply to data which has been derived from personal data. He suggested that targeted advertising profiles

should not contain raw, web-browsing data, but could contain the inferences derived from the data, such as demographic information. He stated that the law passed in Utah does not provide consumers with the right to correct inaccuracies in personal data, and he recommended the inclusion of this language in the proposed bill.

MR. HARKINS asked the committee to consider the role of consent in the proposed legislation and suggested that sensitive data should be governed by opt-in consent. He offered examples of sensitive data associated with geolocation and biometric information. He stated that GDPR and the law in Colorado provide this protection, and that the law in California provides for notice and the right to opt-out. He asked the committee to consider how to define a set of activities which pose a heightened risk to consumers, and once defined, consumers should be provided with the ability to exercise choice or consent regarding the same. He offered that the proposed bill should emphasize opt-out provisions regarding the sale or exchange of data, though the sale and exchange of data for targeted advertising may extend to data associated with, whether a consumer is fit for insurance, housing, or credit, or not. He suggested that these profiles exist regardless of whether they are exchanged or sold. He suggested that the phrasing in the bill may result in some competitive advantage.

1:56:17 PM

REPRESENTATIVE SNYDER referenced the National Research Act, which protects human subjects in biomedical and behavioral research and provides guidelines for the ethical conduct of research. She suggested that data collected may be used to develop AI to predict consumer behaviors or group associations, and this data could have been collected to analyze human behavior. She stated that the Institutional Review Boards (IRBs) protect privacy and offer guidelines for those seeking approval to conduct research. She asked whether the National Research Act has been used to inform the development of privacy legislation and whether there exists any overlap.

MR. HARKINS stated that ethical concerns are relevant to permitting the use of data for public research, even in the furtherance of the public interest. He stated that other laws have been passed which attempted to address these concerns. He offered that a "carve out" could exist for data to be used in an institutional setting, consistent with ethical considerations. He stated that he could not answer whether the National Research

Act has informed the debate on consumer privacy laws. He expressed the opinion that the privacy laws have been more closely associated with FIPPs and the EU's Data Protection Directive. He stated that GDPR has been the leader and primary foundation for discussion.

2:00:56 PM

CHAIR CLAMAN asked why states are not more closely aligned with GDPR, since it is the "gold standard" for international privacy laws.

MR. HARKINS offered that GDPR has a completely different orientation. He explained that GDPR and the Data Protection Directive assume that personal data may not be processed unless there is a demonstrated good reason for doing so. He explained that GDPR outlines that a company, or "controller," which intends to collect and use or share personal data, is required to establish a lawful basis for doing so. He stated that such bases include consent and legitimate interest, which balances the benefits against the risks to a consumer. He added that the orientation of GDPR appears to be "foreign" to most U.S. audiences. He offered that, in the U.S., there is an assumption that one may process data unless one is told that one may not. He offered that there are similarities in other respects, such as the distinction of entities which are subject to the law and their obligations to comply, and similarity in the distinction between controllers and processors, and those who process data only for controllers. He stated that the laws in Colorado and Virginia have adopted the controller/processor model, while California uses the terminology of "business" and "service provider."

MR. HARKINS explained that other similarities include those of consumer rights. He stated that GDPR has a "consent right" which correlates to "opt in," and a "right to object." He stated that a "right to object" is the same as an "opt out." He added that each member state in the EU has its own data protection agency responsible for implementing and enforcing data protection in its country. He stated that California has also created a data protection agency; however, creating a new agency is costly. Other states have declined to create agencies, relying instead on their attorneys general to develop and enforce regulations.

2:05:59 PM

CHAIR CLAMAN asked whether GDPR has a private right of action provision or whether this concept is only in the U.S.

MR. HARKINS responded that the private right of action is more of a concept in the U.S., although individuals may file suit under data protection laws in the EU. He stated that the EU does not have an equivalent to class-action liabilities and suits as the U.S.

REPRESENTATIVE EASTMAN asked how HB 159 would achieve its jurisdiction, applying to some businesses but not to others.

MR. HARKINS answered that HB 159, like other bills, would establish thresholds, with the law applying to companies of a certain size or to those that process a certain amount of data for a certain number of consumers. He added that the threshold may also include companies which process sensitive data for a low number of consumers. He stated that the goal of such thresholds is to try to ensure small businesses are not unduly burdened. He expressed uncertainty on an optimal set of thresholds which would cover the businesses that process a large amount of data and the small businesses that sell data. He pointed out the example of Cambridge Analytica, which is a small business, despite having very sensitive data on a very large number of people. He offered to participate in discussions to aid in establishing thresholds which may meet the committee's priorities. He offered that thresholds could include a percentage of revenue from the sale of data.

2:10:53 PM

REPRESENTATIVE EASTMAN stated that the definition of "business" in the statute does not include nonprofits. He asked how the proposed bill would apply to nonprofits which deal with personal data.

MR. HARKINS answered that some nonprofits process very large amounts of data. These nonprofits would be defined as entities which process the personal information of 100,000 consumers or households, or more, or that derives more than 50 percent of its annual revenue from selling or sharing personal information. He suggested that the decision to apply the law to nonprofits would be one of policy. He noted that the same personal-data-handling risks involve nonprofit as for-profit businesses.

REPRESENTATIVE EASTMAN asked Mr. Harkins what reasons Microsoft Corporation has for supporting this type of legislation.

MR. HARKINS answered that, because there exists growing distrust among consumers and customers regarding personal information, Microsoft has been calling for comprehensive privacy legislation since 2005. He stated that, if the concerns are not addressed in law, some people may elect to not use technology, and, because of the growing distrust, laws could be passed which interfere with responsible data management and innovation. He stated that it is in the best interest of the industry and consumers to create clear rules to regulate, use, and share personal data.

2:14:54 PM

REPRESENTATIVE EASTMAN questioned the number of Alaskans which would be protected by the passage of the bill. He questioned how the proposed legislation would apply to businesses operating outside of the state.

MR. HARKINS answered that, if a company is processing the data of Alaskan consumers, the proposed legislation would apply. He stated the Alaska Consumer Protections Act would add protection along with protections in the state's constitution; however, no comprehensive data privacy protection laws exist in Alaska. In response to a follow-up question, he stated that, if a company is collecting personal data of Alaska consumers online, they are doing business in Alaska. He continued that, if companies are collecting or processing personal information of Alaska consumers, then Alaska may pass a law to regulate this activity.

2:18:37 PM

CHAIR CLAMAN, in relation to consumer protection, questioned the private rights of action compared with enforcement by attorneys general in the different states.

MR. HARKINS explained that California is the only state to allow consumers to sue for data breaches resulting from negligent security practices. He suggested the committee consider the discussions in other states when drafting legislation which includes a private right of action. This could include injunctive relief, actual damages, or attorney fees. He noted that consternation has been expressed among members of the industry concerning large damage awards for cases in which no actual harm had occurred. He suggested that the committee consider the creation of a data privacy commission, as done in California and Washington. This would allow a state agency or

administration to enforce the law via administrative hearings, and this would eliminate the need to file a lawsuit in court.

REPRESENTATIVE EASTMAN noted that the proposed bill would impose a 3 percent tax on revenue from selling or sharing data. He questioned the calculation regarding shared data.

MR. HARKINS responded that concerns exist regarding attempting to calculate and levy a tax on these transactions. He stated that the proposed bill devises an opt-out provision regarding the selling, sharing, or disclosure of information. He offered his interpretation that the language is both too broad and too narrow. He suggested that the bill defines "personal information" broadly enough to cover online data sets based on basic computer information, such as an operating system; however, allowing individuals to opt-out of disclosing such information could implicate data related to navigating from one website to the next. He questioned whether the committee would want an opt-out provision for information which is necessary to make the internet work. He added that some of that information is not being used to profile consumers. He explained that California's law addresses cross-context behavioral advertising, or targeted advertising. He stated that the proposed bill would allow individuals to opt out of sharing this type of data. He stated that third-party sharing of data is one way cross-context behavioral advertising is developed, but this data exchange could also occur directly from a first party. He stated that including a provision regarding third-party data collection and exchange, while not including the same for a first-party collection, could allow for a loophole for a competitive advantage for the largest platforms on the internet.

2:27:10 PM

REPRESENTATIVE EASTMAN asked how the bill differs from other states regarding the role of the attorney general. He stated that Alaska's attorney general is appointed and not elected, and would be permitted to draft regulations, which he suggested would be tantamount to an appointed official writing law.

MR. HARKINS offered that the Virginia's attorney general does not have rulemaking authority, but in Colorado and California, the attorney general does. He added that the rulemaking authority in California is set to transfer to the newly created state data protection agency. He stated that this rulemaking authority is an effort to address laws regulating technology which could ossify quickly as technology evolves. He offered

that one benefit of the rulemaking authority would be to allow a regulatory body, such as an attorney general, to keep up with the pace of technology. He stated that the attorneys general in Colorado and California are elected officials, and he allowed that limiting rulemaking authority for an appointed official to discrete areas of the law could be considered.

CHAIR CLAMAN commented that some challenges exist in the state with fully staffing the attorney general's criminal and civil divisions. He expressed hesitation in adding additional burden to the office, which could be a factor when considering a right of private action provision. He mentioned the federal provision allowing a qui tam lawsuit, by which an attorney general would receive notice and shall decide whether to file suit so that a citizen may bring a private right of action. He asked whether any states had considered this approach to the private rights of action.

MR. HARKINS offered that the legislature in Washington State discussed proposals to allow consumers to file suit after review by a proposed data commission, which would determine whether the consumer had suffered actual harm, and he noted that no such law has been passed.

CHAIR CLAMAN observed that the hearing has revealed information underscoring the complexity of the proposed bill.

[HB 159 was held over.]

2:32:26 PM

ADJOURNMENT

There being no further business before the committee, the House Judiciary Standing Committee meeting was adjourned at 2:32 p.m.