2021 HOUSE INDUSTRY, BUSINESS AND LABOR

HB 1330

2021 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee
Room JW327C, State Capitol

HB 1330
2/9/2021

Prohibiting covered entities from selling users' protected data without consent.

(10:41) Chairman Lefor opened the hearing.

Representatives	Attendance
Chairman Lefor	P
Vice Chairman Keiser	P
Rep Hagert	P
Rep Jim Kasper	P
Rep Scott Louser	P
Rep Nehring	P
Rep O'Brien	P
Rep Ostlie	P
Rep Ruby	P
Rep Schauer	P
Rep Stemen	P
Rep Thomas	P
Rep Adams	P
Rep P Anderson	P

Discussion Topics:

- Internet privacy.

Rep Kading~District 45. Attachment #6098.

Pat Ward~Representing ND Title Insurance Co introduced Nick Hacker.

Nick Hacker~President of ND Title Insurance Co. Attachment #5991.

Matt Gardner~ND Greater Chamber testified in opposition.

Samantha Kersul~TechNet. Attachment #5689.

Levi Andrist introduced Josh Fisher.

Josh Fisher~Alliance for Automotive Innovation-Director of State Affairs. Attachment #5740.

Lisa McCabe~Director State Legislative Affairs-cita. Attachment #5828.

Jordan Crenshaw~Executive Director & Policy Counsel-US Chamber of Commerce. Attachment #5917.

Andrew Kingman~State Privacy & Security Coalition-General Counsel. Attachment #5992.

Al Stenjum introduces Sarah Ohs.

Sarah Ohs~Director of Government Affairs-Consumer Data Industry Association (CDIA). Attachment 6000.

Rose Feliciano~Internet Association. Attachment #6003.

Chairman Lefor closed the hearing.

Rep Louser moved a Do Not Pass.

Rep Adams second.

Representatives	Vote
Chairman Lefor	Y
Vice Chairman Keiser	Y
Rep Hagert	Y
Rep Jim Kasper	A
Rep Scott Louser	Y
Rep Nehring	Y
Rep O'Brien	Y
Rep Ostlie	Y
Rep Ruby	Y
Rep Schauer	N
Rep Stemen	Y
Rep Thomas	Y
Rep Adams	Y
Rep P Anderson	Y

Vote roll call taken Motion carried 12-1-1 & Rep Louser is the carrier.

Additional written testimony: #5702, 5878, 5914, 5915, & 5968.

(11:44) End time.

Ellen LeTang, Committee Clerk

REPORT OF STANDING COMMITTEE

HB 1330: Industry, Business and Labor Committee (Rep. Lefor, Chairman) recommends **DO NOT PASS** (12 YEAS, 1 NAY, 1 ABSENT AND NOT VOTING). HB 1330 was placed on the Eleventh order on the calendar.

Mr Chairman and members of the committee. HB 1330 addresses internet privacy.

Internet privacy is becoming increasingly important in this day and age of data collection and proliferation of the use of such data. Personalized advertising is utilized to a greater extent every year. To big tech linking an individual with specific data is extremely profitable as they can use the data to sell. The issue isn't whether we wish to allow big tech to use aggregate data, the issue is whether we want to allow big tech to use personalized data.

What this bill simply does is require that if big tech wants to sell data that they have scraped from the internet about the everyday person, permission must be obtained from that person. Now this data isn't just basic information such as sex, race, job, and so forth. I am talking about very personal information like browsing history, health conditions, religious affiliations, drug use and so on.

All this bill provides is that a consumer must opt in to allow a big tech company to sell their personalized data. For example if big tech was collecting information about a persons drug use, health condition, or entire browsing history; the big tech giant would have to allow the user to opt in to allowing the sale of information regarding each of those types of information. This doesn't mean every time big tech sells the information, the person has to authorize the sale, this just means that when the person signs up, they have to opt in to allowing such sale. Big tech might say if you don't opt in you don't get to use the site. I think this is appropriate, it is the choice of the consumer. Now perhaps big tech doesn't currently sell every single website every one of you in here has every visited, but have no doubts, this is something without a law like this, they will be doing. Who knows maybe they are already selling each and everyone of our entire browsing histories. They certainly have the ability to do it.

In the bill there are approximately 24 categories of protected information. If you as a committee don't like anyone of them, feel free to amend things in our out.

Ultimately this bill simply provides reasonable protection for the small consumers. Opting in to allowing the sharing of personal data is certainly reasonable. We as representatives represent the everyday person. The

everyday person doesn't have the ability to follow every one of these bills as closely as the lobbyist. The lobbyists following behind me who represent big tech diligently track these issue and are looking to protect the interestes of big tech. The lobbyist following behind my might argue that California regulations or federal regulations are a better approach. I doubt most of you here would agree California or the federal government promulgates better regulations than North Dakota. Despite their elegant arguments to not implement protections for the small guy I urge this committee to pass this bill forward with a do pass to protect the everyday citizen in North Dakota.

House Industry Business and Labor Committee
Hearing on HB 1330

Testimony from North Land Title Association
Nick Hacker – Legislative Chair
nick@thetitleteam.com
(240) 688-2210

Chairman Lefor and Members of the Committee, my name is Nick Hacker with the North Dakota Land Title Association as well as President of North Dakota Guaranty and Title Co.

Our industry provides abstracting, title insurance and real estate closing services in every county of the state. Our job is to ensure buyers acquire real property as they expect, free and clear of liens and to protect lenders on their mortgage should a borrower default occur.

As title insurance agents, we rely on "title evidence" to be able to examine the real property records and eliminate title issue's and risks prior to issuing the insurance policy. "Title evidence" includes abstracts with an attorney's title opinion and prior title insurance policies. A prior title insurance policy reflects the condition of title as reflected in the public records at the County after the policy was purchased. We use these to streamline the time it takes to close on real estate transactions. We do not in the traditional sense collect and sell our customers data.

Due to the vague nature of the bill which does not exempt public records and covers "insurance", this bill would require us to contact thousands of individuals that purchased an insurance policy years ago if we acquired copies of those policies from other title agencies. Even though, all the information on the title insurance policy is already a public record. These insurance policies are assets to our members to provide speed of service and savings to consumers.

Please give this bill a do not pass recommendation.

Thank you.

TechNet Northwest | Telephone 206.791.6407
www.technet.org | @TechNet

TECHNET
THE VOICE OF THE INNOVATION ECONOMY

February 5, 2021

Honorable Chair Mike Lefor
Industry, Business, and Labor Committee
North Dakota State Legislature
600 East Boulevard
Bismarck, ND 58505-0360

Re: TechNet Opposition to HB 1330, concerning data privacy

Honorable Chair Lefor and Members of the Industry, Business and Labor Committee:

TechNet is the national, bipartisan network of technology companies that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50 state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents more than three million employees in the fields of information technology, e-commerce, clean energy, gig and sharing economy, venture capital, and finance. TechNet is committed to advancing the public policies and private sector initiatives that make the U.S. the most innovative country in the world.

I am writing today on behalf of our membership in respectful opposition to HB 1330, concerning data privacy. TechNet members are fully committed to securing privacy and security for consumers, and engage in a wide range of practices to provide consumers with notice, choices about how their data is used, as well as control over their data. We believe this is an unnecessary bill which would cause burdensome challenges for both consumers as well as businesses of all sizes.

North Dakota has already analyzed and rejected the need for state privacy legislation through an interim study process which took place over the last two years. Through that open stakeholder process, this body decided that a federally-led data regulation effort is preferable to a one-state approach. Having one federal privacy standard brings uniformity to all Americans, regardless of where they live, while ensuring that consumers' privacy and security are protected.

Additionally, HB 1330 proposes a significantly different privacy framework from anything that has already passed or is currently being considered nationwide. New privacy laws should provide strong safeguards to consumers while also allowing the industry to continue to innovate. In the absence of federal action, any new proposals should be based upon a uniform set of standards to avoid imposing a patchwork of policies across jurisdictions. Our member companies are already complying with privacy standards established in the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). As a result of this patchwork approach, businesses of all sizes would be forced to create an entirely different compliance structure just to comply in North Dakota. This is costly, time consuming, and difficult for businesses in North Dakota, especially after already investing significant resources to comply with other laws.

HB 1330 will not effectively protect consumers and leads to complications that can impede innovation, we ask you to vote no. Thank you for your ongoing engagement on this important issue. I am available at your convenience should you have any questions.

Best Regards,

Samantha Kersul
Executive Director, Northwest
TechNet
skersul@technet.org
360-791-640

February 6, 2021

The Honorable Mike Lefor
Chair, House Industry, Busines and Labor Committee
State Capitol
600 East Boulevard
Bismarck, ND 58505-0360

RE: HB 1330 - RELATING TO PROHIBITING COVERED ENTITIES FROM SELLING USERS' PROTECTED DATA WITHOUT CONSENT
POSITION: OPPOSE

Dear Representative Lefor:

The Alliance for Automotive Innovation[1] (Auto Innovators) is writing to inform you of **our opposition to HB 1330**, which seeks to impose broad, yet exceptionally vague, requirements on business as it relates to consumer privacy. This bill goes beyond what other states have done and would create competing and conflicting state-level requirements when a federal standard is needed. Given that this issue was studied during the interim and a decision was made not to pursue the issue during the legislative session we request the bill not be advanced.

Maintaining Consumer Privacy and Cybersecurity
The protection of consumer personal information is a priority for the automotive industry. Through the development of the "Consumer Privacy Protection Principles for Vehicle Technologies and Services," Auto Innovators' members committed to take steps to protect the personal data generated by their vehicles. These Privacy Principles are enforceable through the Federal Trade Commission and provide heightened protection for geolocation data and how drivers operate their vehicles.[2] The auto industry's Privacy Principles already prohibit the sale or sharing of sensitive data (including location data) in the absence of affirmative consent.

---

[1] Formed in 2020, the Alliance for Automotive Innovation is the singular, authoritative and respected voice of the automotive industry. Focused on creating a safe and transformative path for sustainable industry growth, the Alliance for Automotive Innovation represents the manufacturers producing nearly 99 percent of cars and light trucks sold in the U.S. The newly established organization, a combination of the Association of Global Automakers and the Alliance of Automobile Manufacturers, is directly involved in regulatory and policy matters impacting the light-duty vehicle market across the country. Members include motor vehicle manufacturers, original equipment suppliers, technology and other automotive-related companies and trade associations. The Alliance for Automotive Innovation is headquartered in Washington, DC, with offices in Detroit, MI and Sacramento, CA. For more information, visit our website http://www.autosinnovate.org.

[2] https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf

1050 K Street, NW
Suite 650
Washington, DC 20001

AutosInnovate.org

With increasing vehicle connectivity, customer privacy must be a priority. Many of the advanced technologies and services in vehicles today are based upon information obtained from a variety of vehicle systems and involve the collection of information about a vehicle's location or a driver's use of a vehicle. Consumer trust is essential to the success of vehicle technologies and services. Auto Innovators and our members understand that consumers want to know how these vehicle technologies and services can deliver benefits to them while respecting their privacy. Our members are committed to providing all their customers with a high level of protection of their personal data and maintaining their trust.

Practical Concerns

With this in mind, we have significant concerns with the proposed legislation. First, HB 1330 lacks clear definitions and clarity about its scope and intent. This bill does not define key terms such as "sale," or "collect"—critical definitions that determine the scope of the bill.

Second, the legislation is overly restrictive. It prohibits the sale of information even if the information is not identifiable or otherwise attributable to a particular user, including when data has been aggregated. Furthermore, HB 1330 does not contemplate various scenarios where a consumer gave the consent to the original collector but not a business which acquired that data from the original collector. California considered adopting similar requirements but rejected the idea.

Third, the bill creates a private right of action. Businesses may very well find themselves in a position of facing severe penalties for even very minor and inadvertent infractions and where there are no actual damages.

Automotive Specific Concerns

While the concerns noted above apply across all industries, their impacts raise unique problems for vehicle manufacturers. There is no provision on how HB 1330 might be applied to information that is collected on a vehicle and not immediately accessed by the manufacturer but could be accessed by the business at some point in the future. Automakers use vehicle-level data they collect for analysis related to motor vehicle safety, performance, and security to comply with the standards set forth by NHTSA. Moreover, this data is crucial to the development, training, implementation, and assessment of automated vehicle technologies, advanced driver-assistance systems, and other life-saving vehicle technologies.

Automakers may need to share information with affiliate companies within the organization and suppliers that focus on specified tasks within the manufacturing ecosystem, such as R&D, manufacturing, and warranties. If automakers are prohibited from sharing such information internally, that would negatively result in automakers not being able to use the information to develop, test, and deploy vehicles and technologies that will save lives.

In addition, automakers, independent dealerships, and suppliers share information for purposes that benefit consumers and the public. Automakers may share information with dealerships and others for safety, security, warranty, or other purposes. California realized the importance of this and subsequently amended their law to not allow consumers to opt-out of 'selling' or sharing to a third party when it is shared for the purpose of vehicle repair related to a warranty or a recall.

Thank you for your consideration of the Auto Innovators' position. Please do not hesitate to contact me at jfisher@autosinnovate.org or 202-326-5562, should I be able to provide any additional information.

Sincerely,

Josh Fisher
Director, State Affairs

February 9, 2021

Oppose House Bill 1330
House Industry, Business and Labor
Chairman Mike Lefor

Dear Chairman Lefor and Members of the House Industry, Business and Labor Committee:

On behalf of CTIA®, the trade association for the wireless communications industry, I write to you in opposition to House Bill 1330. This bill raises particular concerns because its requirements would (1) clash with existing privacy protections, potentially creating consumer confusion, (2) mandate an onerous opt-in framework for the "sale" of "protected data"--concepts that are undefined or vague and/or overly broad, and (3) impose a significant compliance burden, particularly for small- and medium-sized companies. These concerns are even more alarming due to the enormous class action liabilities businesses could face under this bill. With per-user damages of up to $100,000 per violation, the class action provisions in this bill could bankrupt businesses.

The bill creates inconsistencies with existing legislation and protections, potentially resulting in consumer confusion and notice fatigue. Consumer privacy protections should be conceptually and operationally consistent. HB 1330 instead relies on new concepts and frameworks with little basis in existing privacy laws. Most importantly, the definition of "protected data" is not clearly limited to data that is personal in nature and therefore goes beyond existing privacy laws. For example, under the bill "a user's location" or "internet browsing history" could be considered protected data, even if the data would not be linkable to the underlying user, and even if it has been de-identified. The bill also contains no exclusion for data that is publicly available.

California is the only state to pass a comprehensive consumer privacy law. The CCPA provides an opt-out right for the sale of personal data. HB 1330 requires an opt-in right for North Dakota residents. For companies offering service in North Dakota and California, this would be burdensome and would be the start of an onerous patchwork of regulation across the country, and importantly would confuse consumers who would be confronted with overlapping and contradictory privacy protections as they interact with companies.

Users could also experience "notice fatigue" and simply approve every request without paying attention to how it affects their privacy rights. For example, if a consumer orders a new phone from a wireless provider, or any product from any retailer, it appears that the provider or retailer would need to get consent to share the consumer's address with the postal service or shipper to have the phone delivered. On the whole, the bill's consent requirements could lead

to “notice fatigue,” in which consumers stop paying attention to notices and simply click to approve every request – but businesses would still face the burden of presenting and recording these consents. The burden of complying with this kind of obligation would be tremendous, especially for smaller organizations, and would not provide corresponding consumer benefits.

Furthermore, the bill’s opt-in requirements are vague, overly broad and onerous, resulting in additional consumer confusion and generating potential inadvertent violations by businesses. HB 1330’s opt-in provision requires that companies provide users with the opportunity to opt-in to the “sale” of “protected data,” prohibiting companies from selling protected data “to another person” unless the user affirmatively opts-in. The term “sale” is not defined, and it is not clear whether the term would be limited to an exchange involving monetary consideration or whether companies’ routine sharing of data for a business purpose might inadvertently be swept in. For example, without a definition, the term “sale” could potentially include everyday transfers of information necessary for business purposes, such as the exchange of shipment information from a merchant to a mail carrier for fulfillment of consumer orders or the use of back-office cloud tools or platforms for purely internal purposes. Similarly, the bill’s framework could potentially cover the transmittal of location information from a ride sharing application to its drivers who are independent contractors.

Additionally, the term “person” is not defined, and it is not clear whether transfers of protected data between related or affiliated companies could be considered a sale. Without definitions for these terms, companies may reach widely varying conclusions regarding what the bill requires, resulting in inadvertent costly violations by businesses making good faith attempts to comply, as well as creating additional confusion for consumers.

The bill would impose significant compliance burdens, especially on small- and medium-sized businesses, with no evidence of benefit. Broad opt-in consent requirements provide little evident benefit to consumers and are burdensome, if not infeasible, for businesses to implement. This would be particularly true for HB 1330, which would theoretically apply in the same fashion to “protected data” no matter how it is collected – whether online, over the phone, or in person. For example, a call center could potentially be required to obtain opt-in consent for each “type” of protected data the call center collects in order to fulfill a consumer request, requiring call center agents to work through a significant and lengthy script to effectuate opt-in consent. As another example, physical retailers could be required to obtain opt-in consent from customers that walk into physical locations, requiring those retailers to develop a prescriptive compliance program for customer-facing staff that are responsible for collecting protected data.

HB 1330 differs from existing privacy regimes, some of which contain “thresholds” for application (e.g., annual gross revenue minimums, maintaining personal data from a

minimum number of consumers), by applying to businesses both small and large. In other words, a company with a single physical retail location and tens of thousands of dollars in revenue would be subject to the same compliance regime as a company with millions of dollars in revenue and dedicated privacy staff.

The lack of clarity in the bill will expose businesses making a good faith effort to comply to tremendous financial liability. The "penalties" provisions of the bill would impose unprecedented levels of potential liability on businesses and would be especially harmful for small and medium businesses. The bill would provide for statutory damages for violations of at least $10,000 for each user (plus reasonable attorneys' fees), or $100,000 for "knowing" violations (again, for each user). Given the lack of clarity in the bill, even businesses that make a good faith attempt to comply could face catastrophic penalties that could potentially force them to shut down. Businesses may consider such levels of liability and risk unacceptable and decline to start or continue doing business in North Dakota.

As mentioned, California is the only state to enact a comprehensive privacy law and it is still a moving target. It became effective Jan 1 2020; AG enforcement began July 1, 2020. Clarifying bills were passed by legislature in 2019 and 2020. And now with the passage of the ballot measure Prop 24 in November, the California Privacy Rights Act, (CPRA) further changes to the law are being made with new requirements effective in 2023. Accordingly, we caution North Dakota and any state from rushing to follow California down this unproven, untested, and unknown path. Protecting personal data is a national and global issue.

CTIA members are strongly committed to protecting the privacy of their customers, and CTIA supports uniform, technology-neutral consumer privacy protections. Federal legislation is the only way to ensure clear, consistent privacy protections for consumers and certainty for businesses. Neither consumers nor businesses benefit from the fragmentation that additional privacy laws at the state and local levels introduce. As such, CTIA opposes HB 1330 and respectfully urges the committee not to move this bill.

Sincerely,

Lisa McCabe
Director, State Legislative Affairs

#5917

Statement of the Chamber Technology Engagement Center

ON: HB 1330 Data Privacy Bill

TO: North Dakota House Industry, Business & Labor Committee

DATE: February 9, 2021

1615 H Street NW | Washington, DC | 20062

BEFORE THE NORTH DAKOTA HOUSE INDUSTRY, BUSINESS & LABOR COMMITTEE
Hearing on HB 1330 Data Privacy Bill
Testimony of Jordan Crenshaw
Executive Director & Policy Counsel, Chamber Technology Engagement Center

February 9, 2021

Good morning, Chairman Lefor and Vice Chairman Kesier, and members of the Committee. My name is Jordan Crenshaw and I am the Executive Director & Policy Counsel the U.S. Chamber of Commerce's Technology Engagement Center ("C_TEC"). C_TEC was established to promote the role of technology in our economy and to advocate for rational policies that drive economic growth, spur innovation, and create jobs.

At issue today is HB 1330, a proposed data privacy bill that would require all kind of companies to obtain consent before selling personal information to be enforced by potential class action lawsuits. HB 1330 comes at a time when a patchwork of state privacy laws is emerging which threatens to create confusion for both consumers and business, particularly small enterprises. The U.S. Chamber of Commerce supports national privacy legislation that protects all Americans equally and discourages state legislation that could create regulatory uncertainty by imposing enforcement mechanisms like private rights.

I. DATA IS ESSENTIAL TO THE 21ST CENTURY ECONOMY

First, I would like to note that data is transforming our economy and has been vital in keeping the "digital lights on" for many companies, particularly small businesses during the COVID-19 pandemic whether that be through contact tracing, enabling faster distribution of PPP loans by fintech companies, or helping Americans stay connected through remote work, e-commerce, online learning, and telehealth.[1] Prior to the pandemic, C_TEC released a report which showed that even as the number of data breaches increases, identity theft is holding at around the same levels. This is in part due to data being used to identify fraud and stop it in its tracks.[2] We've also found that data used by the private sector is helping protect citizens from wildfires, promote financial inclusion, and enhance public safety. Private-sector data enabled law enforcement to locate and stop the San Bernardino mass shooter during his spree.[3]

What these examples show is that data is necessary to a functioning 21st century society. Privacy legislation should include exceptions for important societally beneficial purposes such as anti-money laundering and fraud protection, research, and commercial credit reporting. Unfortunately, HB 1330 provides **NO** exceptions to its privacy requirements.

---

[1] *America's Next Tech Upgrade: Data For Good and the Need for a National Data Strategy*, C_TEC (Oct. 21, 2020) *available at* https://americaninnovators.com/wp-content/uploads/2020/10/CTEC_TechUpgrade_Data_.pdf.
[2] *Data Flows, Technology, & the Need for National Privacy Legislation*, C_TEC (July 11, 2019) *available at* https://americaninnovators.com/research/data-flows-technology-the-need-for-national-privacy-legislation/.
[3] *Data for Good: Promoting Safety, Health, and Inclusion*, C_TEC (Jan. 30, 2020) *available at* https://americaninnovators.com/wp-content/uploads/2020/01/CTEC_DataForGood_v4-DIGITAL.pdf.

II. The Growing State Patchwork

a. California

A growing patchwork of state privacy legislation and laws currently threatens the ability of companies like retailers, manufacturers and small businesses to innovate and offer services to their consumers. In 2018, California passed the nation's first sweeping privacy legislation.[4] Among rights to access data and deletion, the CCPA gives consumers the right to opt out—not opt in—of data sales.

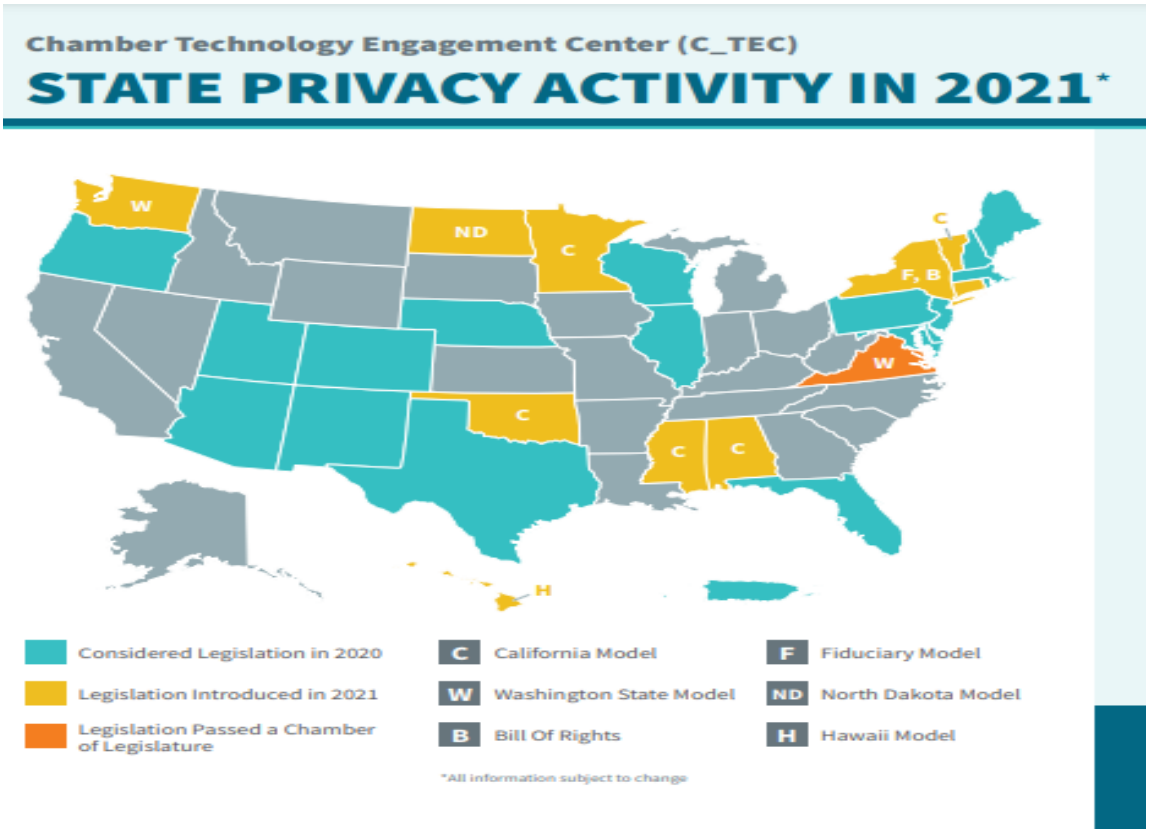
Prior to implementation of CCPA, the State's Attorney General commissioned a study to determine the economic impact its proposed regulations would have on California. According to the study, CCPA regulations could cost State businesses a total of ***$55 billion*** in compliance costs. For businesses with 20 or fewer employees, the regulations are expected to cost small businesses up to ***$50,000***. These costs do not include potential lost revenue or heightened costs from having to administer a complex compliance system that addresses conflicting state laws. Also, California's law does not include a private right of action to enforce its privacy provisions which would further skyrocket economic costs. Californians recently adopted the California Privacy Rights Act, which will become effective in 2023 and will add further costs.

b. Other States

Various state models are currently emerging that could create confusion for Roughrider State consumers and companies doing business across state lines. Several models are emerging[5]:

- **Washington Model:** The "Washington Privacy Act" would give consumers the right to access, correction, deletion, and opt out of processing data for targeted advertising, data sales, and profiling in furtherance of decisions producing a legal effect. Controllers must issue a privacy notice, limit collection and use, and maintain reasonable security. The Attorney General would be tasked with enforcement and the Act would not give rise to a new private right of action. A previous version of the bill nearly passed in 2020 but was defeated because lawmakers in Olympia attempted to pass a private right of action. Lawmakers this year in Virginia overwhelmingly have voted to pass a similar bill.
- **Fiduciary Model:** Among other requirements, the fiduciary model imposes a duty upon companies not to process data in a way that is harmful to consumers.
- **Bill of Rights Model:** Being considered in New York, this model would task the Secretary of State through rulemaking to develop a Privacy Bill of Rights including but not limited to the right to data protection, access, correction, deletion, control, and opting out of sales. A new Data Privacy Advisory Board would provide guidance.
- **Hawaii Model:** This model would require opt-in consent only for internet browser history and location data.

[4] Cal. Civ Code § 1798.100 *et al.*
[5] https://americaninnovators.com/news/2021-data-privacy/



One major takeaway from the various state models is that all the major models neither impose a strict opt-in regime for data sharing nor do they lack exceptions for societally beneficial uses of data. Additionally, California voters approved privacy rules solely enforced by government agencies and legislators in both Washington State and Virginia have rejected private rights of action.

III. Federal Legislation

Lawmakers on Capitol Hill in Washington are also considering national privacy legislation. Most of the privacy bills offer the rights of access, transparency, deletion, and even correction of personal information. Proposals from Republican Senators Roger Wicker (R-MS) and Jerry Moran (R-KS) do not have blanket opt-in requirements that lack permissible uses of data. For example, Senator Wicker's SAFE DATA Act only requires opt-in for sensitive data. Both Republican bills reject a private right of action and create a national privacy standard.[6] Democratic proposals though, except for legislation by Rep. Suzan Delbene (D-WA), would enforce privacy through private rights of action.[7] Even these Democratic proposals, although relying on opt-in for sensitive data recognize the importance of exceptions for legitimate uses of data.

[6] https://americaninnovators.com/wp-content/uploads/2020/10/CTEC_RepFedPrivacyProposals_v1-1.pdf.
[7] https://americaninnovators.com/wp-content/uploads/2020/10/CTEC_RepFedPrivacyProposals_v1-1.pdf

IV. U.S. Chamber Principles for Privacy Legislation

To encourage consumer protection, instill business certainty, and promote innovation, C_TEC calls on Congress to pass national privacy legislation that gives consumers the right to know how data is used, collected, and shared; delete personal information; and opt out of the sharing of personal data that does not have a legitimate purpose. Rights to delete and opt out should take into consideration a business's need to retain and use information as necessary to conduct operations and meet other state and federal requirements such as record retention laws. Privacy legislation should focus solely on personal information that directly identifies a person or can reasonably be used to identify a person.

National Privacy legislation should among other things incorporate the following principles[8]:

- **One National Framework:** Consumers and business benefit when there is certainty and consistency regarding regulations and enforcement of privacy protections. They lose when they must navigate a confusing and inconsistent patchwork of state laws.

- **Risk-Focused and Contextual Privacy Protections:** Privacy protections should be considered in light of the benefits provided and the risks presented by data and by the manner in which it is used. These protections should be based on the sensitivity of the data and informed by the purpose and context of its use and sharing. Likewise, data controls should match the risk associated with the data and be appropriate for the business environment in which it is used. For instance, like the CCPA's approach, personal information collected and otherwise used in an employment and business-to-business context should be exempted from the scope of a national privacy law.

  A national privacy law should enable legitimate uses and promote uses of data that are a net societal benefit and should not hamper critical data processing. For example, privacy legislation should:

  - Permit commercial credit reporting, a service which can be a lifeline for small businesses during COVID-19.

  - Respect First Amendment-protected activities and not inhibit the use and sharing of publicly available data.

  - Facilitate activities to combat malicious or illegal activity like financial crimes, fraud, identity theft, and money laundering; prevent shoplifting; and mitigate security threats. The private sector should continue to be able to assist law enforcement address violations of federal, state and local laws.

- **Transparency:** Businesses should be transparent about the collection, use, and sharing of consumer data and provide consumers with clear privacy notices that businesses will honor.

[8] U.S. Chamber Privacy Principles *available at* https://www.uschamber.com/sites/default/files/023546_ctec_data_privacy_principles_one_pager_02_2019.pdf.

Legislation should not cause the required level of transparency to undermine or eliminate existing trade secret protections.

- **Enforcement Should Promote Efficient and Collaborative Compliance:** Consumers and businesses benefit when businesses invest their resources in compliance programs designed to protect individual privacy. In order to provide certainty and utilize already-existing expertise, federal data privacy legislation should not be enforced by newly created data protection agencies.

  Congress should encourage collaboration as opposed to an adversarial enforcement system. A reasonable opportunity for businesses to cure deficiencies in their privacy compliance practices before government takes punitive action would encourage greater transparency and cooperation between businesses and regulators. In order to facilitate this collaboration, a privacy framework should not create a private right of action for privacy enforcement, which would divert company resources to litigation that does not protect consumers. Enforcement authority should belong solely to the appropriate federal or state regulators.

  According to a report by the U.S. Chamber's Institute for Legal Reform, a private right of action would have negative impacts and [9]:

  - Undermine appropriate agency enforcement and allow plaintiffs' lawyers to set policy nationwide, rather than allowing expert regulators to shape and balance policy and protections

  - Result in inconsistent and dramatically varied, district-by-district court ruling

  - Lead to grossly expensive litigation and staggeringly high settlements that disproportionately do not benefit individuals whose privacy interests may have been infringed

  - Hinder innovation and consumer choice by threatening companies with frivolous, excessive, and expensive litigation, particularly if those companies are at the forefront of transformative new technology.

V. CONCLUSION

Consumers deserve to have their privacy protected in addition to reaping the health, financial, and safety benefits data provides to society. For these companies to most successfully innovate consumers must trust personal information is protected and not have to navigate a confusing patchwork of laws to enforce their privacy rights. It is for this reason that the Chamber believes one robust federal law that protects all Americans equally, enables beneficial uses of data, and is enforced by a clearly identifiable government agency is the correct approach. Thank you for your time and the Chamber is ready to assist as North Dakota continues to consider privacy legislation.

[9] https://instituteforlegalreform.com/research/ill-suited-private-rights-of-action-and-privacy-claims/

STATE PRIVACY & SECURITY COALITION

February 9, 2021

Oppose House Bill 1330
House Industry, Business and Labor
Chairman Mike Lefor

Dear Chairman Lefor and Members of the House Industry, Business and Labor Committee,

The State Privacy and Security Coalition, a coalition of 29 leading telecommunications, technology, retail, payment card, automobile, and online security companies, as well as seven trade associations, writes in opposition to HB 1330. The bill contains a blanket opt-in provision that will frustrate consumers, does not define key terms (and confusingly defines others), and is not interoperable with other state privacy laws. The inclusion of a Private Right of Action, instead of AG enforcement, would contradict other omnibus consumer privacy laws' enforcement provisions and lead to a torrent of frivolous class action litigation.

Importantly, we note that this state's legislature commissioned a comprehensive legislative interim study of data privacy, and concluded after significant deliberation that this was not the right time to attempt this sort of complex regulation at a statewide level. We would urge the legislature to follow this recommendation and not advance HB 1330.

Opt-In Framework

This bill goes far beyond what the Federal Trade Commission's Privacy Framework recommends companies implement. The Framework recognizes that opt-in consent is very important to provide in cases where companies may be handling sensitive data (e.g., health information or precise geolocation information), but that generally, consumers should be given choices within the context of the transaction, because it helps them understand what they are assenting to or opting out of.

The requirements in this bill would inundate consumers with notices that, in practical terms, would create unnecessary burdens for the ordinary course of business for transactions that have no impact on a consumer's privacy. What happens if a company changes cloud storage providers and consumers do not consent? What happens if a business changes payroll processors and an employee doesn't consent?

Even many privacy advocates oppose opt-in consent provisions such as this, because the consumers lose the ability to distinguish between what decisions about their data require extra attention and what decisions are routine operational transactions.

Finally, many of the data elements – such as professional history and residence details - listed in the definition of "protected data" are publicly available. Exemptions for publicly available information are found in nearly every privacy law in the nation, and this is a concept supported by the FTC framework.

Private Right of Action

The data shows that private rights of action – with their inevitable class action lawsuits - are not effective remedies for consumers. In a study[1] of consumer federal class action matters filed in the Northern District of Illinois from 2010-12, researchers concluded that "the cost of using the consumer

[1] *High Cost, Little Compensation, No Harm to Deter: New Evidence on Class Actions Under Federal Consumer Protection Statutes*, Columbia Business Law Review (2017).

class-action procedural device to compensate such a small fraction of consumer class members outweighs the aggregate amount delivered as compensation to consumers." Moreover, "the aggregate amount that class members typically receive comprises a small fraction of the nominal or stated settlement amount. Since courts base attorneys' fees on [this amount]…***attorneys' fees often equal 300%-400% of the actual aggregate class recovery***." (emphasis added). The study concluded that "the findings here confirm the view that class-action settlements are more effective in transferring money from the defendant to class counsel than in compensating class members."

Definitions

- **"Covered Entity":** the definition of "covered entity" would apply to any legal entity in the state, meaning that these new regulations would saddle small businesses with the same costs as larger businesses. Combined with the omitted and unclear definitions we identify below, this would have a significantly negative effect on the state's small businesses. In a post-COVID-19 landscape, we believe that the priority should be on resuscitating the state economy, not imposing additional compliance costs on businesses.
- **"Protected Data":** This definition is not found anywhere else in any state law in the nation. One of the hallmarks of state privacy legislation is the need for interoperability, ensuring that as much as possible, entities that conduct business across state lines are able to implement similar rules. This definition is not tied to any of the major frameworks that exist in other states, and is both overinclusive (for instance, the number of followers someone has is not particularly sensitive) and underinclusive (excluding other types of data that could be reasonably linkable to consumers). Additionally, the definition includes data elements that, for many companies or in many uses, would be covered by existing federal laws such as the Fair Credit Reporting Act.
- **"User":** This definition does not confine the scope of the bill to North Dakota residents. This would raise immediate dormant commerce clause issues upon passage, raising doubts about whether the bill would be enforceable at all.
- **"Opt-In," "Sale,"** and **"Collect":** These are two critical terms in the bill, as they determine the scope of information covered, the activities prohibited, and the type of transfers regulated. However, they are not defined and as such, would likely create dramatically different interpretations among businesses, which would lead to inconsistent application of the bill and ultimately, significant consumer confusion.

We request that HB 1330 not advance. We believe that it is inconsistent with national data privacy standards, would frustrate consumers, and is in fact inconsistent with this legislature's own conclusions just six months ago.

Respectfully submitted,

Andrew A. Kingman
General Counsel
State Privacy and Security Coalition

Sarah M. Ohs
Director of Government Relations
sohs@cdiaonline.org
(202) 408-7404

Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

WWW.CDIAONLINE.ORG

February 7, 2021

The Honorable Mike Lefor
Industry, Business, and Labor Committee
North Dakota State Capitol
600 East Boulevard
Bismarck, ND 58505-0360

Re: CDIA Opposition to HB 1330, concerning data privacy

Dear Chairman Lefor:

I write on behalf of the Consumer Data Industry Association (CDIA) to express our opposition to House Bill HB 1330, an act concerning consumer privacy. Although, this bill strives to create privacy legislation aimed at protecting consumers. As drafted, it has the potential to create significant unintended consequences that could undermine privacy and data security for consumers in North Dakota.

The Consumer Data Industry Association (CDIA) is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals, and to help businesses, governments and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity, helping ensure fair and safe transactions for consumers, facilitating competition and expanding consumers' access to financial and other products suited to their unique needs.

We believe the solution to privacy concerns are best handled at the federal level rather than a patchwork of privacy regulations by the states. The federal government has regulated data privacy for decades and has taken a thoughtful approach in recognizing the different types of data collected and the different uses of that data at the sectoral level. This is important because not all sectors collect the same type of data or use it in the same manner. Therefore, it is difficult to apply a single regulatory standard that governs the uses of all data without potentially creating harmful, unintended consequences.

Fair Credit Reporting Act

All of our members are regulated under the Fair Credit Reporting Act (FCRA). The FCRA outlines the purposes for which a consumer report may be furnished to a requestor. Under the

FCRA, consumers have the right to access all information in their credit reports, including the sources of the information, and the right to disclosure of their credit scores. A consumer may request one free credit report, from each of the nationwide credit reporting agencies (CRAs). Consumers have the right to dispute the completeness or accuracy of information contained in their files.

Beyond providing information that allows individuals to access credit, insurance, screening for employment, the information contained in consumer credit reporting databases aid in many other ways. Location services is one of the ways our members' databases assist law enforcement and state agencies. For example, when police are trying to locate a fugitive or a witness to a crime, they will often rely on one of our members' databases to find a more accurate address to locate the individual.

Fraud Prevention is another way that CDIA members' data are beneficial to states. Prevention of unemployment fraud, workers' compensation fraud and tax fraud are a few areas where this data can be useful. For example, when an individual applies for unemployment benefits with a state, the state labor department can contract with one of our member companies and have the ability to do a search to see if that individual has W2 information reported elsewhere and is working. This can prevent fraud against the state. The same is true if someone has applied for workers' compensation benefits from the state, the individual's name can be searched by one of our members' databases to see if they are working elsewhere. Tax fraud is another area, someone could have the ability to claim a tax exemption in one state but when compared with our members' records one could find if the individual was living elsewhere and claiming that as a primary residence.

Unintended Consequence of Opt-In Provisions

An example of potential harm that HB 1330 fails to recognize is applying an "opt- in" to fraud prevention databases. Companies that provide essential information to government and law enforcement to assist with fraud prevention, such as prevention of unemployment fraud, workers' compensation fraud and tax fraud would be subject to a consumer's ability to delete their information from those databases by choosing not to "opt-in". The consequence of this would be that our member companies could no longer offer fraud prevention services to state agencies, without first tipping off the individual in question, who was potentially trying to defraud the state. In addition, if a consumer has objected to a service provider processing their personal data, it is much easier for that person to encounter identity fraud. This is because the information used to verify the individual would no longer be available in our members' databases as a resource to confirm one's identity. Thus, making it easier for someone to steal another's identity. These are just a few of the examples of how this bill is problematic.

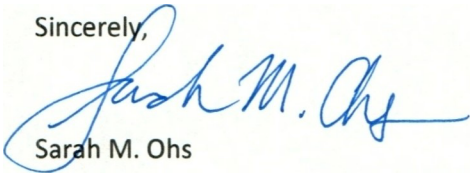
In 2019-2020 CDIA participated in the North Dakota legislature's interim study on data privacy. After careful consideration the committee rejected the need for a new state-led privacy regulation, preferring to leave the discussion at the federal level. The committee recognized that a patchwork of state privacy laws has the potential to harm small businesses and consumers in North Dakota. CDIA continues to have similar concerns regarding HB 1330 that we outlined during the legislature's interim study on data privacy.

Summary

Our members take very seriously the concerns of privacy and data security and use data fairly, responsibly and thoughtfully. There is a long history of privacy regulations federally at the sectoral level that considers the unique needs of data used in each industry. I would encourage you to distinguish between these unique uses of data, and whether or not new regulations are necessary. Existing federal statutes govern most uses of data and how it is gathered, collected and disseminated. A bill that attempts to create one regulation, that is applied across all sectors, fails to distinguish the unique uses of data, and the existing federal statutes that regulate differing industries.

For these reasons above, we respectfully oppose HB 1330. Thank you for your consideration of our comments. I would be happy to answer any further questions the Committee might have.

Sincerely,



Sarah M. Ohs

Director of Government Relations

February 9, 2021

The Honorable Mike Lefor, Chair
House Committee on Industry, Business & Labor
North Dakota State Legislature
Bismarck ND

RE: Internet Association's Opposition to HB 1330.

Dear Chair Lefor and Members of the Committee:

Internet Association (IA) appreciates the opportunity to provide feedback on HB 1330. While IA agrees consumers should have meaningful and easily understood controls over their personal information, we do not believe this proposed legislation is the most effective mechanism to do so.

IA represents more than 40 of the world's leading internet companies and advances public policy solutions that foster innovation, promote economic growth, and empower people through the free and open internet.

IA companies know that trust is fundamental to their relationship with consumers. Our member companies recognize that to be successful they must meet consumers' reasonable expectations about how the personal information they provide to companies will be collected, used, and shared. That is why our member companies are committed to transparent data practices, and are continually refining their consumer-facing policies to ensure they are clear, accurate, and easily understood by all consumers.

IA is concerned about the implications of HB 1330 due to its broad language and lack of clearly defined terminology. The definition of "protected data"only includes a list of vague terms that are considered "protected data," but does not further define words such as "child" or "interests." This will lead to covered entities being confused as to which information is protected under the proposed chapter. For example, the federal Children's Online Privacy Protection Act (COPPA) defines a child as 13 years or younger, but without a definition of "child" it would be impossible for a covered entity to appropriately identify a child and their information.

Moreover, the term "sale" is consistently found throughout the bill. However, the bill's definition section does not include what actions are considered a "sale" under this chapter. Without a definition, this creates a great deal of uncertainty for covered entities that are required to provide an opt-in mechanism for users before their "protected data'' is sold. Additionally, in the absence of clear guidance about whether a user needs to be notified with an opt-in prompt before or after the protected data is sold creates confusion for covered entities to implement this requirement under the chapter, and does not create a stable way for users to know when their information is being sold.

IA strongly opposes the inclusion of a private right of action (PRA) as the primary enforcement mechanism. Instead, IA member companies believe that the most effective way to enforce a consumer's state privacy rights is through the state's attorney general.

For these reasons, IA strongly recommends you not move this bill out of committee. I appreciate your consideration. If you have any questions please do not hesitate to reach out at 206-326-0712 or rose@internetassociation.org

Sincerely,

Rose Feliciano
Director, Northwest Region, State Government Affairs

AT&T

Cheryl Riley
President, External Affairs
Northern Plains States

AT&T Services, Inc.
3709 W. 41st St.
Sioux Falls SD 57106

M: 307.365.1379
CR6557@att.com
www.att.com

#5702

February 9, 2021
Oppose House Bill 1330
House Industry, Business and Labor
Chairman Mike Lefor

Dear Chairman Lefor and Members of the House Industry, Business and Labor Committee:

On behalf of AT&T, I want to encourage the committee to oppose HB 1330. This legislation is sweepingly broad and vague, extraordinarily difficult to implement, burdensome and costly to North Dakota businesses.

In 2019-2020, the North Dakota legislature commissioned a legislative interim study of data privacy. After examining the findings, North Dakota rejected a state-led privacy or data regulation effort, opting to allow the federal discussion to continue.

Since the internet is not constrained or governed by state borders, a patchwork of conflicting state privacy legislation is problematic and impractical. Through extensive study, we've already collectively determined that such legislation would be burdensome for North Dakota consumers and businesses alike.

Risks of HB 1330

- **Burdensome Compliance Rules**: HB 1330 is significantly different than other privacy or data sales bills, such as the California Consumer Privacy Act (CCPA) or the General Data Protection Regulation (GDPR). It would force businesses to create an entirely new and different compliance structure. This would make compliance difficult, costly and time consuming for businesses in North Dakota, many of which have already invested significant time and resources to comply with other privacy laws. It would also impose additional compliance costs on businesses still reeling from the pandemic.

- **Unclear Definitions and Lack of Interoperability:** This bill does not define key terms such as "sale," or "collect"—critical definitions that determine the scope of the bill. Additionally, the bill does not clearly delineate how "protected data" elements like credit and banking information would interface with established federal law like the Fair Credit Reporting Act and Gramm-Leach-Bliley Act, which already regulate many of these data points.

- **Unworkable Opt-Ins**: Other states have rejected opt-ins as ineffective. As drafted, the bill requires opt-in consent for every single potential transaction. Consumers already have notification fatigue; this bill would create even further challenges and frustrations for consumers.

- **Unnecessary Private Right of Action**: North Dakota already allows for the Attorney General to bring regulatory actions against companies that engage in unfair or deceptive business

practices. Private rights of action (PRA) encourage unnecessary litigation and could lead to negative, unintended consequences for consumers and North Dakota businesses of all sizes. PRAs take valuable time and resources from businesses that might otherwise be spent on creating jobs and investing in innovation. Most of all, they are unnecessary due to existing consumer protection tools which provide appropriate and consistent checks and penalties against the theft or misuse of consumers' personal data.

Federal legislation would not only ensure consumers' rights are protected, but it would also provide consistent rules of the road for all internet companies, across all websites, content, devices and applications.

National, clear privacy standards would allow consumers to keep using the services they love and keep the U.S. at the forefront of innovation with burgeoning technologies like autonomous vehicles, the Internet of Things and advanced agriculture technologies.

For all these reason, AT&T opposes HB 1330 and encourages the committee to reconsider this legislation and follow the recommendations of the interim study.

Sincerely,

Cheryl Riley
AT&T President, External Affairs
Northern Plains States

Gabby Reed, Manager
State Government Affairs – Rocky Mountain Region

Elsevier
LexisNexis Legal & Professional
LexisNexis Risk Solutions
Reed Exhibitions

February 8, 2021

The Honorable Mike Lefor
North Dakota State Capitol
600 East Boulevard
Bismarck, ND 58505-0360

Re: House Bill 1330 "Relating to prohibiting covered entities from selling users' protected data without consent"

Dear Chairman Lefor and Members of the House Industry, Business and Labor Committee:

I am writing on behalf of RELX and LexisNexis to express our strong opposition to House Bill 1330 "Relating to prohibiting covered entities from selling users' protected data without consent". Although the bill aims to grant consumers additional rights pertaining to the sale of protected data, House Bill 1330 would result in a myriad of unintended consequences for North Dakota consumers, businesses, and the state economy. RELX/LexisNexis urges you to review the findings of the Interim Commerce Committee's study of protections, enforcement, and remedies regarding the disclosure of consumers' personal data that took place in 2019 and 2020. The Interim Commerce Committee ultimately rejected a state-led privacy or data regulation effort.

LexisNexis is a division of RELX and is a leading provider of business information, including fraud prevention and identity verification services, for Fortune 1000 businesses, government and law enforcement agencies, and the property and casualty insurance industry. LexisNexis plays a vital role in supporting government, law enforcement, and business customers who use our information services for important uses including: detecting and preventing identity theft and fraud, finding deadbeat parents or missing children, locating suspects, and preventing and investigating criminal and terrorist activities.

***

Below is a sample of the negative consequences that would result if House Bill 1330 became law:

The bill would create an **incredibly burdensome regulatory regime** that is sweepingly different than other established privacy frameworks such as the California Consumer Privacy Act (CCPA) or the General Data Protection Regulation (GDPR), both for which companies have already invested valuable time and resources to ensure compliance. The result of establishing yet another compliance framework would be extremely costly, in both time and resources, for North Dakota Businesses, especially after these businesses have already gone through an exhaustive implementation process to ensure compliance with existing laws.

Furthermore, this new regulatory regime would require an **unworkable opt-in requirement** for every single potential transaction. It is important to note that existing consumer privacy regulation frameworks have accepted opt-out provisions as the most consumer-friendly mechanism to exercise control over their personal data. Especially in areas such as fraud prevention, consumer data could not be used for fraud prevention solutions unless they have proactively opted-in, something they may be unlikely to do due to prevalent notification fatigue. Thus, such a requirement would hurt legitimate consumers as their data could not be used for fraud prevention measures.

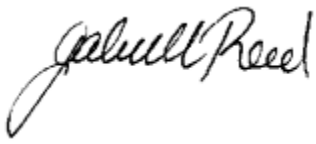
House Bill 1330 would also directly **result in costly litigation** for North Dakota companies, even those complying with the provisions of the law in good faith. A private right of action is never a productive penalty for regulatory compliance issues as it takes time and resources that would be better spent on creating jobs and investing in innovation. Additionally, a private right of action is not appropriate as enforcement tools already exist including the ability of the Attorney General to bring regulatory actions again companies that engage in unfair or deceptive business practices.

***

The issues outlined above provide just a few examples of how House Bill 1330 would create a disastrous regulatory environment for North Dakota consumers and businesses. RELX encourages the committee to recognize the comprehensive work already completed by the Interim Commerce Committee that ultimately rejected pursuit of a state-led privacy or data regulation effort.

Thank you for your consideration of RELX's concerns pertaining to House Bill 1330. Should you have any questions, please do not hesitate to contact me either via e-mail at gabby.reed@relx.com or at 202-403-7893.

Sincerely,



Gabby Reed
Manager, State Government Affairs - Rocky Mountain Region
RELX Group

February 8, 2021

The Honorable Chairman of the House Industry, Business and Labor Committee
Representative George Keiser
422 Toronto Drive
Bismarck, ND 58503-0276

The Honorable Vice Chairman of the House Industry, Business and Labor Committee
Representative Mike Lefor
P.O. Box 564
Dickinson, ND 58602-0564

RE: North Dakota HB 1330

Dear Chairman Keiser and Vice Chairman Lefor:

On behalf of the digital advertising industry, we provide the following comments on North Dakota's HB 1330.[1] As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country, from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising spend. We and the companies we represent strongly believe consumers deserve meaningful privacy protections.

We also believe in the importance of maintaining a thriving Internet and information-driven economy, where robust innovation drives strong economic growth, employing millions of Americans and providing transformative benefits for consumers. These objectives are not mutually exclusive. It is vital that consumer privacy legislation appropriately supports these key goals. North Dakota, along with the United States as a whole and the rest of the world, has borne witness to a historic economic downturn and a significant uptick in unemployment due in large part to the COVID-19 pandemic.[2] At a time when we all face some of the most challenging circumstances in recent history, legislation that threatens to increase financial strain on companies can have the unintended effect of forcing businesses to divert important resources away from maintaining employment levels in order to address sweeping new legal requirements. We encourage the North Dakota legislature to carefully consider the impacts privacy legislation could have on businesses and how such impacts may harm consumers if legislation is not reasonably tailored to work for both consumers and businesses in the state.

---

[1] HB 1330 (N.D. 2021), located at https://www.legis.nd.gov/assembly/67-2021/documents/21-0816-02000.pdf.
[2] *See* BISMARCK TRIBUNE, *Midwest economy improving but businesses less optimistic; North Dakota loses 33,000 nonfarm jobs* (Jan. 5, 2021), located at https://bismarcktribune.com/business/midwest-economy-improving-but-businesses-less-optimistic-north-dakota-loses-33-000-nonfarm-jobs/article_1f47b865-317d-5d66-8354-10f393e486fd.html; *see also* NORTH DAKOTA STATE UNIVERSITY, Center for the Study of Public Choice and Private Enterprise, *Economic Outlook*, located at https://www.ndsu.edu/centers/pcpe/research/economic_outlook/.

I. HB 1330 Should Not Adopt an Opt-In Consent Requirement

North Dakota should not adopt a one-size fits all consent requirement for the sale of protected data. No other state has taken this approach. Such an approach would create the most restrictive privacy law in the United States, thereby hindering legitimate business, particularly small businesses, and harming North Dakotan consumers. We recommend that the legislature initiate a study to examine various approaches to data privacy so that North Dakotans can benefit from a careful analysis of proposed privacy provisions as well as experiments in other jurisdictions.

If the House of Representatives elects to move forward now, it should eliminate the bill's opt-in consent requirement. HB 1330 states that "[a] covered entity may not sell a user's protected data to another person unless the user opts-in to allow the sale."[3] The bill also requires a user to be "given the opportunity to opt-in to the sale of each type of protected data by individual selection."[4] Though the bill does not provide a definition of "sale," the term "protected data" is defined broadly to include a user's interests, shopping habits, and Internet browsing history, among a number of other data elements.[5] Requiring opt-in consent for transfers of such information would unreasonably burden North Dakotans and would severely limit their ability to access important information and resources for free or at a low cost. We therefore encourage the legislature to revise HB 1330's flat prohibition on sales of covered data absent opt-in consent by instead adopting a more nuanced approach to empowering consumers to control sales of protected data.

While we fully support consumers' ability to control sales of protected data associated with them, requiring opt-in consent for such transfers could reduce North Dakotans' ability to access important information and services online. In privacy proposals and laws across the United States, as well as the General Data Protection Regulation in Europe, opt-in consent requirements are reserved for the most sensitive data. However, HB 1330 would extend an opt-in consent requirement to a much broader swath of data elements, many of which have been found to not be sensitive, such as a user's professional history, screen name, and purchase history. As described in further detail in Section III below, data transfers power the online economy and enrich consumers' lives by providing them with free and low-cost access to crucial content, news, research, products, and services provided by businesses. The free flow of data is imperative for the Internet ecosystem to function, and consumers benefit greatly from this existing structure. Moreover, HB 1330's requirement that consumers opt-in to the sale of *each type of protected data by individual selection* would place an enormous burden on North Dakotans to approve transfers of discrete data elements included in the protected data definition.

We strongly believe the legislature should amend HB 1330 to enable consumers to opt out of protected data sales rather than require them to opt in to such sales. This amendment would align HB 1330 with the prevailing approach taken in other state privacy laws as well as industry self-regulatory programs and codes of conduct, such as those administered by the Digital Advertising Alliance ("DAA"). Opt-in consent requirements hinder consumers' ability to

[3] HB 1330, Section 1, Prohibition against sale of protected data except with consent.
[4] *Id*.
[5] *Id*.

access vital online resources. We encourage the North Dakota legislature to revise HB 1330's prohibition on sales of protected data absent user consent by instead enabling consumers to opt out of personal data sales.

II. Enforcement for Violations of HB 1330 Should be Vested in the Attorney General Alone

As presently drafted, HB 1330 enables private citizens to bring actions against covered entities for violations of the bill.[6] HB 1330 also expressly allows for class action lawsuits.[7] We strongly believe that the responsibility for enforcing violations of privacy laws should be vested in the North Dakota Attorney General ("AG"), and HB 1330 should not include a private right of action or allow for class action lawsuits. We encourage the legislature to amend the bill's enforcement provisions so enforcement is within the purview of the Attorney General alone. This adjustment would lead to strong outcomes for consumers while better enabling covered entities to allocate funds to developing processes, procedures, and plans to facilitate compliance with the new data privacy requirements set forth in HB 1330.

If HB 1330 is enacted with a private right of action, North Dakota would be adopting the most aggressive privacy law enforcement approach in the United States. The private right of action in HB 1330 is more expansive in scope than any other state privacy law that has been enacted to date, including the California Consumer Privacy Act of 2018 ("CCPA").[8]

Incorporating a private right of action in HB 1330 would create a complex and flawed compliance system without tangible privacy benefits for consumers. Allowing private actions would flood North Dakota courts with frivolous lawsuits driven by opportunistic trial lawyers searching for technical violations, rather than focusing on actual consumer harm. Private right of action provisions are completely divorced from any connection to actual consumer harm and provide consumers little by way of protection from detrimental data practices.

Additionally, including a private right of action in HB 1330 would have a chilling effect on the state's economy by creating the threat of steep penalties for companies that are good actors but inadvertently fail to conform to technical provisions of law. Private litigant enforcement provisions and related potential penalties for violations represent an overly punitive scheme that does not effectively address consumer privacy concerns or deter undesired business conduct. A private right of action would expose covered entities to extraordinary and potentially enterprise-threatening costs for technical violations of law rather than drive systemic and helpful changes to business practices. It would also encumber covered entities' attempts to innovate by threatening them with expensive litigation costs, especially if those companies are visionaries striving to develop transformative new technologies.

Beyond the staggering cost to North Dakota businesses, the resulting snarl of litigation could create a chaotic and inconsistent enforcement framework with conflicting requirements based on differing court outcomes. Overall, a private right of action would serve as a windfall to the plaintiff's bar without focusing on the business practices that actually harm consumers. We

[6] HB 1330, Section 1, Violation – Penalties, § 1.
[7] HB 1330, Section 1, Violation – Penalties, § 2.
[8] *Compare* HB 133, Section 1, Violation – Penalties *with* Cal. Civ. Code § 1798.150.

therefore encourage legislators to alter HB 1330's enforcement provisions and refrain from including a private right of action in the bill.

III. The Data-Driven and Ad-Supported Online Ecosystem Benefits Consumers and Fuels Economic Growth

Throughout the past three decades, the U.S. economy has been fueled by the free flow of data. One driving force in this ecosystem has been data-driven advertising. Advertising has helped power the growth of the Internet for years by delivering innovative tools and services for consumers and businesses to connect and communicate. Data-driven advertising supports and subsidizes the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising allows consumers to access these resources at little or no cost to them, and it has created an environment where small publishers and start-up companies can enter the marketplace to compete against the Internet's largest players.

As a result of this advertising-based model, U.S. businesses of all sizes have been able to grow online and deliver widespread consumer and economic benefits. According to a March 2017 study entitled *Economic Value of the Advertising-Supported Internet Ecosystem*, which was conducted for the IAB by Harvard Business School Professor John Deighton, in 2016 the U.S. ad-supported Internet created 10.4 million jobs.[9] Calculating against those figures, the interactive marketing industry contributed $1.121 trillion to the U.S. economy in 2016, doubling the 2012 figure and accounting for 6% of U.S. gross domestic product.[10]

Consumers, across income levels and geography, embrace the ad-supported Internet and use it to create value in all areas of life, whether through e-commerce, education, free access to valuable content, or the ability to create their own platforms to reach millions of other Internet users. In a September 2020 survey conducted by the Digital Advertising Alliance, 93 percent of consumers stated that free content was important to the overall value of the Internet and more than 80 percent surveyed stated they prefer the existing ad-supported model, where most content is free, rather than a non-ad supported Internet where consumers must pay for most content.[11] The survey also found that consumers value ad-supported content and services at $1,403.88 a year, representing an increase of over $200 in value since 2016.[12]

Consumers are increasingly aware that the data collected about their interactions on the web, in mobile applications, and in-store are used to create an enhanced and tailored experience. Importantly, research demonstrates that consumers are generally not reluctant to participate online due to data-driven advertising and marketing practices. Indeed, as the Federal Trade Commission noted in its recent comments to the National Telecommunications and Information Administration, if a subscription-based model replaced the ad-based model, many consumers likely would not be able to afford access to, or would be reluctant to utilize, all of the

---

[9] John Deighton, *Economic Value of the Advertising-Supported Internet Ecosystem* (2017), located at https://www.iab.com/wp-content/uploads/2017/03/Economic-Value-Study-2017-FINAL2.pdf.
[10] *Id*.
[11] DAA, *SurveyMonkey Survey: Consumer Value of Ad Supported Services – 2020 Update* (Sept. 28, 2020), located at https://digitaladvertisingalliance.org/sites/aboutads/files/DAA_files/Consumer-Value-Ad-Supported-Services-2020Update.pdf.
[12] *Id*.

information, products, and services they rely on today and that will become available in the future.[13] It is in this spirit–preserving the ad-supported digital and offline media marketplace while helping to design appropriate privacy safeguards–that we provide these comments.

* * *

Thank you for your consideration of these comments. We look forward to working further with you on refining HB 1330.

Sincerely,

Dan Jaffe
Group EVP, Government Relations
Association of National Advertisers
202-269-2359

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

Christopher Oswald
SVP, Government Relations
Association of National Advertisers
202-269-2359

David Grimaldi
Executive Vice President, Public Policy
Interactive Advertising Bureau
202-800-0771

David LeDuc
Vice President, Public Policy
Network Advertising Initiative
703-220-5943

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

[13] Federal Trade Commission, *In re Developing the Administration's Approach to Consumer Privacy*, 15 (Nov. 13, 2018), located at https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

AD TRADE COMMENTS REGARDING NORTH DAKOTA HB 1330

We are leading national advertising and marketing trade associations comprised of the Association of National Advertisers **(ANA)**, the American Association of Advertising Agencies **(4A's)**, the American Advertising Federation **(AAF)**, the Interactive Advertising Bureau **(IAB)**, and the Network Advertising Initiative **(NAI)**. We collectively represent thousands of companies across the country, from small businesses to household brands, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies, is responsible for more than 85 percent of U.S. advertising spend, and drives more than 80 percent of our nation's digital advertising spend.

COMMENTS ON HB 1330: As described in more detail in the attached letter, we and the companies we represent strongly believe consumers deserve meaningful privacy protections. We also believe in the importance of maintaining a thriving Internet and information-driven economy, where robust innovation drives strong economic growth, employing millions of Americans and providing transformative benefits for consumers. Throughout the past three decades, the U.S. economy has been fueled by the free flow of data. One driving force in this ecosystem has been data-driven advertising. Advertising has helped power the growth of the Internet for years by delivering innovative tools and services for consumers and businesses to connect and communicate. Digital advertising benefits consumers and fuels the economy. It is in this spirit—preserving the ad-supported digital and offline media marketplace while helping to design appropriate privacy safeguards—that we provide these comments.

- **HB 1330 SHOULD NOT ADOPT AN OPT-IN CONSENT REQUIREMENT.** North Dakota should not adopt a one-size fits all consent requirement for the sale of protected data. Doing so would create the most restrictive privacy law in the United States, thereby hindering legitimate business—particularly small businesses—and harming North Dakotans as consumers. We ask the legislature to instead initiate a study to examine potential approaches to data privacy so North Dakotans can benefit from a careful analysis of proposed privacy provisions as well as experiments in other jurisdictions.

- **ENFORCEMENT FOR VIOLATIONS OF HB 1330 SHOULD BE VESTED IN THE ATTORNEY GENERAL ALONE.** HB 1330 should not include a private right of action or allow for class action lawsuits. Incorporating a private right of action in HB 1330 would encourage frivolous lawsuits by opportunistic trial lawyers, hinder innovation and economic development in North Dakota, and create a complex and flawed enforcement scheme without providing tangible privacy benefits for consumers. Such an approach would also create an anti-business environment in North Dakota by exposing companies to potentially enterprise-threatening costs for mere technical violations of the bill. Adopting an Attorney General enforcement framework instead would provide more consistent and reliable protections for North Dakotans and more clear rules of the road for businesses. We ask the legislature to modify HB 1330 to remove the private right of action and class action provisions.

* * *

North Dakota Retail Association

1014 East Central Avenue + PO Box 1956
Bismarck, ND 58502 + 701-223-3370
www.ndretail.org
Fax: 701-223-5004

Testimony- HB 1330

February 9, 2021- House IBL

Chairman Lefor & Members of the House IBL Committee:

For the record, I'm Mike Rud, President of the North Dakota Retail Association. On behalf of NDRA, I'm submitting written testimony asking for a "**DO NOT PASS" recommendation on HB 1330.**

First and foremost, the issue of data privacy continues to garner a lot of national attention. NDRA still stands by its initial position of a well-defined and easy to implement federal law being the most effective route to ensure sound data privacy laws. A patchwork of different state laws will make it very confusing for our members operating in multiple states.

All retail businesses have no higher priority than earning and maintaining trusted relationships with their customers. Our success depends on providing the highest quality goods and services at competitive prices. Customers expect us to protect the information they share with us and use it in a responsible manner to connect them with our products and services.

Government regulation must not restrict the benefits and services customers enjoy in their relationships with Main Street businesses. Those benefits and services are how consumers stretch their dollars and realize tangible benefits. Our coalition believes that state data privacy legislation must:

- Avoid Private Rights of Action and Liability-Shifting – We oppose efforts to delegate principal enforcement of state privacy laws to trial attorneys through private rights of action. We support a safe harbor for first-party businesses to protect them from being held vicariously liable for the privacy violations of other parties.

- Preserve Customer Service, Convenience and Benefits – We support legislation that preserves the ability of consumers and businesses to voluntarily establish mutually beneficial relationships, including rewards and loyalty programs. We support exceptions to the regulation of data sales to preserve common first-party data sharing arrangements that benefit the consumer and do not involve personal information being sold to a third-party for their own use.

- Narrowly Define Personal Information and Related Terms – We oppose legislation that unnecessarily expands what data would be considered "personal information" and legislation that fails to exempt de-identified or aggregated data from this definition. We support excluding any data that would constitute employee data or business-to-business data, where the latter includes data sharing that facilitates transactions between businesses.

- Provide Uniformity and Industry-Sector Neutrality – We support requiring all businesses that handle consumer information to have direct legal obligations under privacy laws and honor consumer privacy rights requests.

Again, NDRA urges a **"DO NOT PASS"** recommendation on HB 1330 .