HB

230

<TARGET><BILL>HB 230</BILL><SUBJECT>HB 230</SUBJECT><COMM>HL&C30</COMM></TARGET>

Representative Harriet Drummond
Sponsor Statement

HB230 Internet Privacy Act

House Bill 230 restricts any telecommunication service or internet service provider from collecting personal information of a private customer without the consent of the customer to protect the privacy and individual liberty of every Alaskan.

Alaska is one of the most independent states in the Union which is reflected by the citizens who live here. In a time of the most technologically advanced society, Alaskans pride themselves on independence, individual liberty and privacy. HB230 will protect privacy of Alaskans' personal information stored on a cyber based utility.

Cell phones, computers, laptops and tablets are all modern tools with which private citizens are able to conduct commerce and trade. Online shopping and bill paying have become very popular with easy accessibility to businesses and providers. Many of these devices have the capability to retain memory of any account number, social security number, credit card information, medical information and online purchases. Passing HB 230 will put into law that telecommunication companies and internet service providers must be given consent by the user of any service or device before selling, trading, or gifting information entered by a private citizen.

HB230 prevents discrimination of users who decline to allow the sharing of personal information by telecommunication companies and internet service providers. HB230 simply restricts large companies from selling information of a private citizen to the highest bidder without the consent of the user.

Passing HB230 will assure users of cyber connected devices that no information is collected without the express written consent of the user. HB230 keeps Alaskans' information private, preserving the individual liberty and independence of every Alaskan.

Staff Contact: Patrick FitzGerald (907) 465 3875

Representative Harriet Drummond
Section Analysis

House Bill 230 "Internet Privacy Act"

"An act relating to the collection of customer information by telecommunications and Internet service providers; and establishing an unfair trade practice under the Alaska Unfair Trade Practices and Consumer Act"

Sec. 1.

Establishing the collecting of personal information by Telecommunications companies or Internet service providers without the consent of the customer or user of service is considered (1) Effect on public interest (2) Not a reasonable method of conducting or preserving business (3) is an unfair trade and deceptive practice of business operations.

Sec. 2 – AS 45.48 is amended by adding a new section to read:

Article 6A. Information Disclosure

Sec. 45.48.800 Approval required for Information disclosure.

Telecommunications Company or Internet service providers are not allowed to collect personal information without the expressed written approval of the customer. Telecommunications Company or Internet service providers may not discriminate a paying customer solely because a customer denied the right for the Telecommunications Company or Internet service providers to collect information.

Telecommunications Company is defined as Cable, telegraph, telephone, or broadcasting.

Sec. 3 – AS 45.50.471

Adds a new paragraph AS 45.48.800 explaining violation of credit/debit card information sharing now includes Internet and telecommunications providers.

Sec. 4 AS 45.48.800

Definition of "Telecommunication service" and establishes an effective date.

Fiscal Note

State of Alaska
2017 Legislative Session

Bill Version: HB 230
Fiscal Note Number:
() Publish Date:

Identifier: HB230-LAW-CIV-04-28-17
Title: TELECOMMUNICATIONS & INTERNET PRIVACY
Sponsor: DRUMMOND
Requester: House Labor & Commerce

Department: Department of Law
Appropriation: Civil Division
Allocation: Commercial and Fair Business
OMB Component Number: 2717

Expenditures/Revenues

Note: Amounts do not include inflation unless otherwise noted below. (Thousands of Dollars)

	FY2018 Appropriation Requested	Included in Governor's FY2018 Request	Out-Year Cost Estimates				
OPERATING EXPENDITURES	**FY 2018**	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**
Personal Services							
Travel							
Services							
Commodities							
Capital Outlay							
Grants & Benefits							
Miscellaneous							
Total Operating	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Fund Source (Operating Only)

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Positions

Full-time							
Part-time							
Temporary							

Change in Revenues

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimated SUPPLEMENTAL (FY2017) cost: 0.0 *(separate supplemental appropriation required)*
(discuss reasons and fund source(s) in analysis section)

Estimated CAPITAL (FY2018) cost: 0.0 *(separate capital appropriation required)*
(discuss reasons and fund source(s) in analysis section)

ASSOCIATED REGULATIONS

Does the bill direct, or will the bill result in, regulation changes adopted by your agency? No
If yes, by what date are the regulations to be adopted, amended or repealed?

Why this fiscal note differs from previous version:

Not applicable, initial version.

Prepared By: Valerie Rose, Budget Analyst — Phone: (907)465-3674
Division: Administrative Services Division — Date: 04/28/2017 10:46 AM
Approved By: Jahna Lindemuth, Attorney General — Date: 04/28/17
Agency: Department of Law

Fiscal Note

State of Alaska
2017 Legislative Session

Bill Version: HB 230
Fiscal Note Number:
() Publish Date:

Identifier: HB230-LAW-CIV-04-28-17
Title: TELECOMMUNICATIONS & INTERNET PRIVACY
Sponsor: DRUMMOND
Requester: House Labor & Commerce

Department: Department of Law
Appropriation: Civil Division
Allocation: Commercial and Fair Business
OMB Component Number: 2717

Expenditures/Revenues

Note: Amounts do not include inflation unless otherwise noted below. (Thousands of Dollars)

	FY2018 Appropriation Requested	Included in Governor's FY2018 Request	Out-Year Cost Estimates				
OPERATING EXPENDITURES	**FY 2018**	**FY 2018**	**FY 2019**	**FY 2020**	**FY 2021**	**FY 2022**	**FY 2023**
Personal Services							
Travel							
Services							
Commodities							
Capital Outlay							
Grants & Benefits							
Miscellaneous							
Total Operating	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Fund Source (Operating Only)

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Positions

Full-time							
Part-time							
Temporary							

Change in Revenues

None							
Total	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**	**0.0**

Estimated SUPPLEMENTAL (FY2017) cost: 0.0 *(separate supplemental appropriation required)*
(discuss reasons and fund source(s) in analysis section)

Estimated CAPITAL (FY2018) cost: 0.0 *(separate capital appropriation required)*
(discuss reasons and fund source(s) in analysis section)

ASSOCIATED REGULATIONS

Does the bill direct, or will the bill result in, regulation changes adopted by your agency? No
If yes, by what date are the regulations to be adopted, amended or repealed?

Why this fiscal note differs from previous version:

Not applicable, initial version.

Prepared By: Valerie Rose, Budget Analyst — Phone: (907)465-3674
Division: Administrative Services Division — Date: 04/28/2017 10:46 AM
Approved By: Jahna Lindemuth, Attorney General — Date: 04/28/17
Agency: Department of Law

FISCAL NOTE ANALYSIS

STATE OF ALASKA **BILL NO.** HB 230
2017 LEGISLATIVE SESSION

Analysis

This bill would add a new statute, AS 45.48.800, approval required for information disclosure, to AS 45.48 (personal information protection act). If a telecommunications service or internet service provider has entered into certain types of agreements with a state or a municipality, or that uses facilities that are subject to those agreements, the provider (even if not a party to the agreements) may not collect personal information from a customer resulting from the customer's use of the telecommunications service or Internet service without written consent of the consumer.

A violation of AS 45.48.800 would be an unlawful unfair or deceptive act or practice in the conduct of trade or business. The Attorney General is authorized under current law to investigate deceptive trade practices. Also under current law, a person may bring a private action for relief and damages caused by an unlawful act or practice.

The Department of Law currently receives approximately 450 consumer complaints annually alleging unfair or deceptive practices. Of those, approximately 30 complaints or 7% relate to internet transactions or telecommunication services. The department cannot be certain whether the number of complaints the department receives would increase significantly should this bill become law, however, the department anticipates being able to continue to allocate its resources for consumer protection duties within existing staffing levels. Therefore, the department does not expect a fiscal impact if the bill becomes law.

Alaska Telephone Association

Ed Cushing
President

201 E. 56th Avenue, Suite 114
Anchorage, AK 99518
(907) 563-4000
www.alaskatel.org

Christine O'Connor
Executive Director

April 28, 2017

The Honorable Sam Kito
Chair, House Labor & Commerce Committee
State Capitol, Room 403
Juneau, AK 99801

Dear Chair Kito and Members of the Committee,

We are writing to express our concern with HB 230 "An Act relating to the collection of customer information by telecommunications and Internet service providers; and establishing an unfair trade practice under the Alaska Unfair Trade Practices and Consumer Protection Act."

Privacy is a serious and legitimate concern in the online world we all depend on, but HB230 will not provide new protections. Instead it threatens to disrupt essential broadband service for consumers, mandates highly disruptive and burdensome consent requirements for internet users, and will confuse consumers.

This proposed legislation would frustrate, rather than help consumers, and is unnecessary. The reality is that Alaska's telecommunication/ISPs do not sell customer's personal web browsing history. To the contrary we are deeply conscious of the sensitivity of the private information inherent in communications services and are vigilant to protect it. Our privacy policies are posted online and we are available at all times to answer questions from customers. (URLs listed below.) Further, the Federal Communications Commission ("FCC") continues to apply protections under the Communications Act to the privacy practices of ISPs. In 2015, the FCC issued enforcement guidance under section 222 of the Communications Act. This guidance, which continues to apply today, ensures that ISPs are held accountable for unreasonable privacy practices.

HB 230's requirements are not necessary and would annoy consumers by requiring affirmative consent for routine internet functions, and may actually prevent the provision of broadband service. Some level of customer information is required to allow a company to provide and support broadband service. Without personal details needed to provision, support and troubleshoot service, a provider would be unable to deliver broadband despite the proposed statutory language mandating service.

Privacy is a critical priority for customers, providers and policy makers. As the FCC's privacy rules had never gone into effect, the actions taken recently by Congress just maintained the status quo. Following enactment of the congressional resolution, the chairs of the FCC and Federal Trade Commission committed to work together to adopt a consistent federal policy on Internet privacy.

ATA member companies have always been and will continue to be vigilant to protect our customers' privacy. Our customers are our communities, our neighbors and our families and we consider it a privilege to provide broadband service to them. We are excited about the many benefits broadband service brings to Alaskans and ask that HB 230 not be adopted. HB 230 would obstruct our ability to service our customers and communities. We respectfully ask that HB 230 not be advanced.

Respectfully submitted,

Christine O'Connor
Executive Director

Ed Cushing
President

ctia™
Everything Wireless

April 28, 2017

The Honorable Representative Sam Kito
Alaska House of Representatives
Chair, House Labor & Commerce Committee
State Capitol Room 403
Juneau AK, 99801

RE: Opposition to House Bill 230

Dear Chair Kito:

On behalf of CTIA, the trade association for the wireless communications industry, I write in opposition to Alaska House Bill 230, which would restrict how telecommunications and internet service providers (ISPs) operate in Alaska.

Any suggestions that ISPs, including CTIA members, have unique access to consumer data online are unfounded. A comprehensive study by veteran Clinton and Obama Administration privacy expert Peter Swire showed that ISPs actually have limited insight into the online activity of consumers.[1] HB 230 unnecessarily targets one set of providers - telecommunications providers and internet service providers - and treats them differently than others operating in the internet ecosystem.

The wireless industry takes a proactive approach to protect consumer privacy. Our members provide consumers with detailed privacy policies, which clearly describe how providers protect consumer data. Current federal and state statutes also provide additional layers of protection for sensitive consumer information. In addition, telecommunications providers and ISPs, including CTIA members, have recently recommitted to principles that maintain privacy protections consistent with the Federal Trade Commission's effective privacy framework, covering transparency, consumer choice, security, and data breach notifications.[2]

It is important to note that recent Congressional action did not change privacy protections for wireless consumers. The Federal Communications Commission (FCC) rules had not taken effect, so nothing changed from the regulatory framework that has existed for the past two years. Moreover, the framework advocated for by ISPs aligns with that of the Obama Administration, which noted that, "uniform consumer data

---

1 "Online Privacy and ISPs: ISP Access to Consumer Data is Limited and Often Less than Access by Others," http://www.iisp.gatech.edu/sites/default/files/images/online_privacy_and_isps.pdf, Swire, Peter, last accessed 4/28/2017: "ISP access to user data is not comprehensive – technological developments place substantial limits on ISPs' visibility. [And] ISP access to user data is not unique – other companies often have access to more information and a wider range of user information than ISPs."

2 "Protecting Consumer Privacy Online," http://www.ctia.org/docs/default-source/default-document-library/final---protecting-consumer-privacy-online.pdf, last accessed 4/28/2017.

privacy rules are necessary to create certainty for companies and consistent protections for consumers."[3] The current FCC Chairman has also clearly stated that, "[i]nternet service providers have been – and will continue to be – obligated to comply with Section 222 of the Communications Act and other applicable federal and state privacy, data security, and breach notification laws."[4]

HB 230 imposes unjustified restrictions on ISPs and deviates from the privacy framework and standards that have been in place for decades. The proposed language would make it very difficult for ISPs to operate in Alaska and would create inconsistent privacy standards for different parts of the internet ecosystem, which will ultimately confuse consumers and have a host of unintended consequences.

CTIA member companies have long recognized the importance of protecting consumer data and respecting consumer privacy. In 2003, CTIA and the wireless carriers that are signatories to the "Consumer Code for Wireless Service," including AT&T, Sprint, T-Mobile, and Verizon Wireless, made a commitment to help consumers make informed choices.[5] The tenth point of the Code provides that signatory carriers agree to abide by policies for the protection of customer privacy. As part of that commitment, carriers follow policies regarding the privacy of customer information in accordance with applicable federal and state laws and make available privacy policies concerning information collected online. The wireless industry recognizes the importance of customer privacy and takes strong measures to protect customer data.

HB 230 would create two sets of rules that are different for various entities within the internet ecosystem - harming competition and creating consumer uncertainty about which rules apply to their data. Survey results submitted to the FCC last year showed that 94 percent of internet users believe all companies touching their online data should follow the same privacy rules.[6] These findings indicate that HB 230, which targets only ISPs, would not effectively protect consumer privacy because many other companies would continue to collect and use consumer data without being subject to the express written approval requirement.

CTIA members are absolutely committed to protecting consumer information as they value consumer trust. Existing federal and state laws and protections remain intact today rendering the bill unnecessary. Moreover, CTIA members have committed to a

---

[3] "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," http://repository.cmu.edu/cgi/viewcontent.cgi?article=1096&context=jpc, last accessed 4/28/2017.

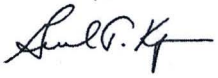
[4] Letter from FCC Chairman Ajit Pai to Sens. Markey, Blumenthal, Warren, Franken at http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0317/DOC-343949A1.pdf, last accessed 4/28/2017.

[5] CTIA Consumer Code for Wireless Service, http://www.ctia.org/initiatives/voluntary-guidelines/consumer-code-for-wireless-service, last accessed 4/28/2017.

[6] The Progressive Policy Institute, "Consumers Want One Set of Rules Protecting Their Information," http://www.progressivepolicy.org/press/press-releases/press-release-consumers-want-one-set-rules-protecting-information/, last accessed 4/28/2017.

framework to protect consumer information and privacy. For these reasons, we respectfully ask that you not move HB 230.

Sincerely,



Gerard Keegan
Assistant Vice President
State Legislative Affairs

cc: Members, House Labor & Commerce Committee
The Honorable Harriet Drummond
The Honorable Scott Kawasaki
The Honorable Les Gara
The Honorable Chris Tuck
The Honorable Justin Parish

April 27, 2017

Honorable Sam Kito
House Labor and Commerce Committee, Chair
Barnes 124
Juneau, AK 99801

Honorable Harriet Drummond
HB 230, Sponsor
Room 108
Juneau, AK 99801

[Sent Electronically for Distribution]

RE: **HB 230** relating to protecting the privacy and security of internet users – **OPPOSE**

Dear Chair Kito and Representative Drummond:

The undersigned associations write to respectfully **oppose HB 230.** This bill, if passed, creates serious unintended consequences and would negatively impact consumers, business and the Internet. It would foster a complicated regulatory structure at the state level for a sector that is best addressed via a national approach. HB 230 would make Alaska a far more difficult place to innovate on the Internet, ultimately hurting the information economy that has become an important part of the state's economy.

The undersigned associations oppose this legislation because it would contribute to an unworkable "patchwork" of state privacy laws, and risks unnecessary harm to the information economy.

Consumers and Businesses Can Rely on the Federal Approach to Privacy. The recent repeal of the Federal Communication Commission's ("FCC") Broadband Privacy Rules does not mean that consumers will be left unprotected. In fact, Internet Service Providers ("ISPs") have been and will continue to be substantially regulated at the federal level. Prior to the FCC's decision to adopt the Broadband Privacy Rules, it issued a wide-ranging enforcement advisory opinion, making it clear that the Communications Act (Section 222) applies to ISPs. This guidance continues to apply today. The recent action by Congress and the President does not change or alter the obligations of ISPs under Section 222, or the FCC's ability to enforce noncompliance. Nor does the recent repeal of the Broadband Privacy Rules create new rights or powers for ISPs because the rules never went into effect. As such, consumers continue to be protected under existing FCC authority.

Following the decision to repeal the FCC's Broadband Privacy Rules, FCC Chairman Ajit Pai announced that the FCC would be working with the Federal Trade Commission ("FTC") to restore the FTC's authority over ISP privacy practices.[1] Chairman Pai reiterated that the FTC is and has been the regulatory leader with respect to privacy, and that we need to "end the uncertainty and confusion that was created in 2015 when the FCC intruded in this space."[2] As indicated by Chairman Pai, consumers need greater certainty and clarity with respect to privacy regulation, and this certainty and clarity will be achieved at the federal level. Greater certainty and clarity will not be achieved through states entering into a regulatory space that has been historically addressed through a national approach.

HB 230 Would Disrupt the Internet and Harm Consumers. HB 230 would greatly exacerbate the growing "patchwork" of state laws on privacy practices. Unlike in other areas, state laws regulating the privacy practices of ISPs would be very difficult for companies to implement and would affect how consumers experience the Internet. This patchwork would force consumers to face a constant drumbeat of confusing and frustrating requests for consent to use the Internet for routine purposes that would vary depending upon the state where the consumer lives. A state-by-state approach, which will vary as each state debates and passes legislation, will inevitably be worse for consumers and organizations. The Internet cannot function as it has if each state is individually regulating how the Internet operates. Such state-by-state legislation would be incredibly disruptive.

The unprecedented growth and success of the Internet over the past two decades, and the high rate of consumer adoption that goes along with it, demonstrates that consumers are pleased with the Internet that has developed under current law. They are increasingly relying on the free and low-cost access to entertainment, news, and financial services, and other useful content that the Internet offers. By destabilizing the ecosystem, HB 230 threatens the "free Internet" that has become part of the daily lives of millions of American consumers.

Advocates for HB 230 and similar bills in other states have failed to identify a single, concrete harm that would be remedied through it. Instead, HB 230 proponents have offered a speculative "parade of horribles" without justification or evidence.

HB 230 Has Not Undergone Adequate Review or Analysis. HB 230 is attempting to regulate in a complicated, highly technical area despite the fact that it has not received sufficient analysis. Prior to enacting the Broadband Privacy Rules, the FCC underwent an extensive rulemaking process, receiving comments from organizations, building a record, and contemplating stakeholder concerns. After a year of regulatory consideration, the FCC released the final Broadband Privacy Rules. HB 230, however, is merely a reaction to the decision to repeal the FCC's Broadband Privacy Rules, and is not the product of a deliberative, thoughtful legislative process.

HB 230 was hastily drafted, was not properly vetted, and, as a result, is poorly constructed. HB 230 has been introduced at the end of Alaska's legislative session, forcing members to move forward without fully understanding the impact of the legislation, and without giving members adequate time to address issues with the language in the legislation.

---

[1] FEDERAL COMMC'N COMM'N, Statement of Chairman Pai on President Signing Cong. Resolution of Disapproval (April 3, 2017), *available at* https://www.fcc.gov/document/statement-chmn-pai-president-signing-cong-res-disapproval.
[2] *Id.*

HB 230 Would Stifle Economic Growth and Innovation. According to the Value of Data report commissioned by the DMA in 2015, the Data-Driven Marketing Economy generated $202 billion in revenue and 966,000 jobs in 2014. Similarly, the Interactive Advertising Bureau ("IAB") commissioned a study, which revealed that the advertising supported Internet ecosystem generated $1.121 trillion for the U.S. economy in 2016, accounting for 6% of U.S. GDP, double its contribution in 2012. The IAB study also noted the advertising-supported Internet ecosystem created 10.4 million jobs in the United States, a 104% increase from 2012. The regulatory landscape for the Internet that existed prior to the FCC's rules helped facilitate these significant economic developments. HB 230 would stifle that growth. A recent Zogby Analytics poll commissioned by the Digital Advertising Alliance ("DAA") shows that consumers assign a value of almost $1,200 a year to ad-supported online content. Ad-supported online content is the backbone upon which the Internet as we know it is built. Altering it or disrupting it would be very harmful to the Internet's role as an economic engine for the American economy.

We have already seen the disruptive effects of restrictive requirements for the Internet in other regions, including Europe. It is no coincidence that the major Internet and technology companies in the world were developed in the United States, under the privacy regime that existed before the FCC's Broadband Privacy Rules were adopted. A state-by-state approach on privacy, such as the one set forth in HB 230, would put the United States in an inferior competitive position and harm the American economy as a result.

Because it is unnecessary for consumers as they already receive significant protections under federal rules, unduly burdens Alaska's businesses (both small and large), and negatively impacts Alaska's tech and data-driven economy, the undersigned associations respectfully oppose HB 230.

Sincerely,

DMA – Data & Marketing Association
4A's – American Association of Advertising Agencies
AAF – American Advertising Federation
ANA – Association of National Advertisers
IAB – Interactive Advetising Bureau
Internet Association
Internet Coalition
NetChoice
TechNet

cc: Honorable Members of the House Labor & Commerce Committee

Internet Privacy: Existing Policies and Consumer Protections

Why did Congress recently act on privacy?

Congress rolled back the Federal Communications Commission's rules because those rules did little to protect consumer privacy and only created confusion and a false sense of security for consumers. The rules fragmented the Federal Trade Commission's unified approach to privacy protection that's been working for 20 years.

Did the vote in Congress impact consumers' internet privacy?

Repeal of the FCC's broadband privacy rules does not harm consumers or change the status quo. Indeed, nothing for consumers has changed because repeal leaves in place the existing legal framework that has been in place for over two years since the FCC adopted the *Open Internet Order* and reclassified broadband Internet access service as a telecommunications service.

What about the FCC rules in the news?

The FCC rules had not taken effect yet. Those rules, had they been implemented, would have put requirements only on internet service providers that were inconsistent with the rules that apply to all other players on the internet who hold much more consumer information than the ISPs. Consumers want regulations that apply to their data consistently no matter what kind of company is holding that data. Consumer information should be protected based on the sensitivity of the information, not the entity collecting it.

Should states take legislative action?

Consumer privacy should be protected consistently across the internet. Policy to ensure robust protection of consumer privacy on the internet should be uniform across the nation and should be enforced by a single government agency. AT&T and every other major internet service provider has committed to additional ***privacy principles***, which are consistent with the privacy framework developed by the Federal Trade Commission (FTC) over the past twenty years. States continue to have the authority to enforce privacy and consumer protection without any need for legislation that could disrupt the Internet and have enormous unintended consequences.

How does AT&T protect privacy?

AT&T's ***privacy protections*** are the same today as they were five months ago when the FCC rules were adopted. The Congressional action had zero effect on the privacy protections AT&T afforded to consumers.

Our privacy commitments are always available on our website:
http://about.att.com/sites/privacy_policy

- We safeguard our customers' data, using encryption and other security techniques to protect it.
- We do not sell your individual web browsing history.
- Medical, tax and financial data is, and has always been, private.
- Our Privacy Policy explains what information we collect, how we use it, and with whom we share it. The Policy is written in plain language and is easily accessible on our website.

AT&T

Privacy: Consumers Remain Protected Under Existing Laws

The recent congressional action repealing the Federal Communication Commission's new broadband privacy rules had no impact on consumer privacy because the rules had not even taken effect yet.

Consumer privacy continues to be protected by robust federal and state privacy laws:

- AT&T remains supportive of robust and consistent privacy protections that apply across the internet.
- The FCC retains enforcement authority over internet providers and requires them to protect their customers' personal information. Internet providers must obtain your permission to sell your web browsing history or sensitive information.
- Health, financial and children's data are further protected under additional federal laws that remain fully in force. Below are just a few examples of these additional protections:
  - The ***Health Insurance Portability and Accountability Act*** (HIPPA) protects your medical records and certain health information.
  - The ***Electronic Communications Privacy Act*** (ECPA) protects the privacy of your electronic communications.
  - The ***Children's Online Privacy Protection Act*** (COPPA) protects data collected from children under age 13.
- Internet providers must also comply with state privacy laws, including data breach notification laws. States continue to have the authority to enforce privacy and other consumer protections without any need for new legislation.

AT&T's commitment to our customers' privacy has not changed:

- AT&T's ***Privacy Policy*** gives you control over your personal information. You can opt out of AT&T using or sharing your data for marketing and advertising programs.
- AT&T and other major internet providers have committed to additional legally enforceable ***Privacy Principles***, which cover data security and data breach notifications, among other things. These principles are consistent with the FTC privacy framework that applies to all other Internet companies, including search engines, ad networks, data brokers and social networks.

Internet privacy laws should apply on a nationwide basis:

- Congress' recent action was not the "last word" on internet privacy laws.
- The chairs of the Federal Communications Commission and the Federal Trade Commission have vowed to ***work together*** to restore the FTC's unified privacy framework to ensure federal privacy laws are effective and consistently applied to all online companies in the internet ecosystem.

AT&T

ACLU
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
Alaska

Myths vs. Facts: The Great Consumer Internet Privacy Debate

Debunking industry objections to privacy-protective bills to prevent Internet Service Providers (ISPs) from collecting and selling sensitive personal information about their customers' internet use without opt-in consent.

Industry Myth #1: Regulating consumer internet privacy protections in Alaska will create a "patch-work" of unworkable laws, rendering ISPs unable to provide consistent service.

Reality: Good Alaska privacy law will help the entire country by raising the standard. The ISPs say it's not workable to institute consumer privacy protections in one state but not in the others. But that makes no sense. Think of how California does environmental regulation, which ends up benefiting the rest of us. When you buy a bottle of shampoo, it might say something about California environmental protection law on the bottle. Companies won't make fifty different types of shampoo; instead, they'll make one version, which conforms to California's high environmental standard. That ends up benefitting the rest of the country, and there's no reason to believe it would work differently with the internet. If Alaska lawmakers pass a consumer internet privacy law, the rest of the country will benefit—confirming our status as a leader in the area of privacy law.

This argument from the ISPs is particularly galling because they lobbied so hard against the FCC (Federal Communications Commission) regulations, which of course would have been uniform across the country. The real reason they don't want this kind of legislation has nothing to do with consistency; it's all about maximizing corporate profits at the expense of consumer privacy protections.

Industry Myth #2: The ISPs don't sell your personal information, and the industry promises to self-police are good enough.

Reality: If the ISPs didn't want to sell your information, they wouldn't be lobbying so hard to stop these straightforward consumer privacy protections from becoming law. If it's really true that the ISPs don't engage in any practices these bills would prohibit, why not codify those practices into law? In no other space do we accept large corporations' promises to self-police, particularly when so much money is on the line. We don't let coal companies self-police when it comes to carbon emissions, and we don't let pharmaceutical companies exchange regulations for promises about drug safety. Consumer internet privacy rules should be no different.

Industry Myth #3: Passing consumer ISP privacy law will hurt Alaskas' businesses or tech economies.

Reality: The proposals don't say anything about start-ups or other technology businesses; they regulate only ISPs. App developers, software companies, and medical device manufacturers will not see any enhanced regulation as a result of law that restricts *an ISP's* ability to sell—without consumer opt-in consent—sensitive customer data. The bills only regulate ISPs, not small start-ups or other technology companies. Talk of "unintended economic consequences" is vague wording for a reason; this language is meant to scare legislators away from doing the right thing. Don't be fooled.

Industry Myth #4: It's not fair to regulate ISPs while letting companies like Google and Facebook off the hook.

Reality: ISPs are not like so-called "edge providers" like Google and Facebook, in that consumers don't have a choice but to use ISPs if they want access to the internet. ISPs are more like phone companies than they are like Google or Facebook. Consumers in Alaska can choose to use Google or Facebook or choose not to. But if they want to use the internet, they must pay an ISP to get online. For that reason, in the 21st century, when everyone relies on the internet to do everything from get jobs to find love, ISPs are like utilities. And just like the government has long regulated utilities, it should regulate ISPs to ensure fairness and privacy online. ISPs are also different from Google and Facebook in that the former charge customers to get online, while Google and Facebook exchange services for user data—not a direct deposit payment or check once per month. Finally, in many places in Alaska, consumers don't have a choice between different ISPs. That anti-competitive environment makes it more important for the state legislature to act.

Industry Myth #5: The federal government and state Attorney General will take care of regulating the ISPs, so there's no need for the legislature to get involved.

Reality: The Trump administration has demonstrated that it has no interest in protecting consumer privacy rights. One of the few things the Trump administration has done since he came into office is gut Obama-era Federal Communications Commission (FCC) privacy rules.

The Federal Trade Commission (FTC) does not have the legal authority necessary to ensure consumers are protected, and in this political climate in Washington, Congress is unlikely to change that. Indeed, Trump's FCC commissioner is now working to kill net neutrality regulations, too—meaning ISPs may soon be able to slow down traffic to certain websites, while speeding up traffic to others. If net neutrality rules are eliminated, it will be even harder for the federal government to hold ISPs accountable for consumer privacy violations.

The ISPs also claim current state law is sufficient because the state AG can sue them for "unfair and deceptive" business practices. But the current state of the law is woefully inadequate to protect consumers in the digital world. Just think about the last time you clicked "I Agree" on a Terms of Service agreement. The deck is stacked against ordinary people, and litigating "unfair and deceptive" practices cases is costly, politically challenging, and legally thorny.

The reason the ISPs are lobbying so hard against these proposals is that they would actually limit the corporations' ability to collect, use, and sell our information without our consent. That's what we need, whether they like it or not. If federal law and AG enforcement provided equivalent protections to the ones in these bills, the ISPs wouldn't mind if we passed a state law resembling the now-gutted FCC rules.