STATE REPRESENTATIVE
TERESE BERCEAU

WISCONSIN STATE ASSEMBLY

77TH DISTRICT

Representative Quinn, thank you for agreeing to hold a public hearing on the important issue of internet privacy.

I've handed out a document that explains what AB 788 does in detail. I'd like to discuss why the bill is needed.

I think the Equifax data breach last fall brought into stark relief how vulnerable our personal information can be. Criminals obtained the names, mailing addresses, e-mail addresses, birth dates, Social Security numbers, driver's license numbers, and credit card numbers and expiration dates for up to 145 million people. The public was frightened and didn't know what to do to protect themselves.

In 2016, the Federal Communications Commission voted in favor of strong consumer protections for broadband users. Internet Service Providers (ISPs) would have to get permission from their customers before they could collect and sell information on which web sites people visit, what apps they use, where they use their devices, and their personal financial and medical data.

Last spring, Congress passed and the president signed legislation to repeal those rules. However, political differences should not stop us from going forward with basic protections for our constituents who are looking to us for help.

AB 788 address privacy issues on the state level because of concerns Congress may not act in a timely manner, or at all. According to the National Conference of State Legislatures, 22 other states have introduced bills to counteract the FCC decision to reduce internet privacy protection.

I'm sure many of you have heard from constituents who do not want their personal, private information amassed, sliced and diced, and sold off to anybody who can afford the asking price set by their ISP. I know I have.

There is a longstanding tradition of protecting privacy in our society. If someone listened to your phone conversations without your knowledge, or read your e-mail or text messages without any valid reason, wouldn't you consider that to be an incredible invasion of your privacy? You would understandably be alarmed if the information obtained through those means could be sold to advertisers or other entities, especially if you didn't know what data was sold or to which companies. So, why are internet providers allowed to track your search history and sell it?

An entire industry has sprung up to sell us programs and services to stop ISPs and search engines from accumulating our user data. But why should we have to pay an ISP for internet access and then also pay to keep our personal information private? As Matt Stamper, a risk/security analyst put it, "What the recent [FCC] ruling has done is effectively change

State Capitol, Post Office Box 8952, Madison, WI 53708 • (608) 266-3784 • FAX: (608) 282-3677
Email: rep.berceau@legis.wisconsin.gov • Web page: www.terese.org

privacy from a right to a commodity that is brokered. Privacy principles emphasize choice and consent; that is, we choose to 'opt-in' and share our information at our discretion. That is now absent."

Law enforcement has to get a warrant, approved by a judge, to search your house, to tap your phones, to access your text messages. Why do internet providers have carte blanche to access this kind of information? We even have a law here in Wisconsin that prohibits anyone from placing a GPS device on someone else' vehicle and tracking that person's movements and location. Yet right now, ISPs can track and sell your virtual movements and location all across the internet.

ISPs will tell you that there are people who really appreciate receiving targeted ads based on their previous search history. I'm not at all certain that it's worth the trade-off though. I get an ad for dog treats after I search for dog food. The ISP gets to mine that data, aggregate it for specific geographic areas or searched items, create social graphs about my habits and who my friends are, and use or sell that information to peddle more products.

Is everyone comfortable with ISPs selling off that in-depth knowledge of who people are and what they like to anybody and everybody without their knowledge or consent? If ISPs merely wanted to target ads to willing consumers, an opt-in procedure would be a win-win by steering ads only to people who are truly interested.

ISPs will tell you it's not fair to target them if we do not also regulate Google and Facebook. But ISPs have much more information on what we do, how often we use our computers, where we use them, have access to our entire browsing histories. They can track what we do across the entirety of the internet. That's significantly more data than Google or Facebook can compile about us.

People also choose whether or not to use Google and Facebook. There are other search engines and social media platforms. If you don't like the business practices of one, you do have the freedom to go to another site.

That's not the case with ISPs. In many parts of Wisconsin, especially rural areas, there is only one ISP. It's either take it or leave it, regardless of how it treats its customers.

The biggest question is why the ISPs are fighting legislation like this. They claim they don't sell any personal data. They must anticipate a market for that information developing in the future if they truly aren't already selling it.

ISPs also claim they collect and combine only meta data so that it isn't personalized. However, according to the Electronic Frontier Foundation, when aggregate information is hacked your chances of becoming a victim of identity theft increase substantially. In addition, according to a report from the Internet Society companies are developing increasingly sophisticated tools that can tie together tremendous amounts of data that don't seem to be related. That makes is easier to "identify individuals – and classes of individuals – from supposedly anonymized or deidentified data."

In addition, ISPs say it's difficult for them to develop programs that would protect privacy. However, American broadband providers are already working on this issue because the

European Union has established strong privacy rules that all members will have to implement, and they are doing business in Europe and with European companies. The EU rules are considerably more extensive than anything required or even envisioned here. They're way ahead of us because they take privacy seriously and have been working on these efforts for over 20 years.

You will hear I'm sure that last December, several months after AB 788 was drafted, the Federal Communications Commission asserted primacy over the states in determining how to regulate net neutrality. That determination apparently also included internet privacy laws.

However, the language used indicated that privacy laws passed by the states would be "extremely limited." That order is expected to be appealed by states that oppose pre-emption of their authority as well as other parties. I have a speaker following me who will address that issue.

There is also conflicting information regarding whether the FCC actually has regulatory authority over broadband. The agency states Congress has withheld that oversight ability, but also claims it does have the ability to pre-empt the states from taking action themselves. The FCC has already lost in court over the pre-emption argument.

Tennessee and North Carolina passed laws to prevent broadband networks owned by municipalities from expanding. The FCC tried to override those laws, but the Sixth Circuit Court of Appeals ruled in 2016 that the FCC didn't have the authority to do so.

Given this complex state of affairs, I believe it behooves us to determine what our constituents want, and move forward. Perhaps our example at the very least will serve as a communication to the FCC on what consumers are hoping to see in personal privacy protection.

STATE REPRESENTATIVE
TERESE BERCEAU

WISCONSIN STATE ASSEMBLY
77TH DISTRICT

- AB 788 prohibits broadband internet service providers from using a customer's proprietary information unless the customer grants the ISP permission
- Different types of approval are required for sensitive and non-sensitive information

Sensitive information

- For sensitive information the customer must grant express affirmative consent after receiving a notification that is required to accompany the provider's request to use the information
- Sensitive information includes
    - Financial information
    - Health information
    - Information pertaining to a child
    - Social security number
    - Precise geo-location information
    - Content of communications
    - And web browsing history and smart phone or tablet application usage history

Non-sensitive information

- For non-sensitive information the customer must object to the provider's request to use the information after the customer receives the company's request
- Non-sensitive information includes:
    - Information that is linked or reasonably able to be linked to an individual or a device; or

State Capitol, Post Office Box 8952, Madison, WI 53708 • (608) 266-3784 • FAX: (608) 282-3677
Email: rep.berceau@legis.wisconsin.gov • Web page: www.terese.org

- Information that identifies an individual and relates to the quantity, technical configuration, type, destination, location, or amount of use of broadband internet access service

Refusal provision

- Under the bill a provider is prohibited from refusing to provide broadband internet access service because a customer does not allow access to their proprietary information

Requirements for provider's request

- when a provider requests approval to use a customer's proprietary information, the provider's request must accompany a notice that includes a specific description of the following:
  - 1) the types of customer proprietary information that the provider will collect and how it will use the information;
  - 2) the circumstances under which the provider discloses or permits access to each type of customer proprietary information that it collects;
  - 3) the categories of entities to which the provider discloses or permits to access the customer's proprietary information and the purposes for which that information will be used by each category of entity; and
  - 4) the customer's rights to grant, deny, or withdraw approval concerning the customer's proprietary information
  - The notice must also include access to a mechanism that the customer can use to grant, deny, or withdraw approval at any time

Material change Provision

- When a provider makes a material change to its policies concerning the privacy of customer proprietary information, the provider must give to each customer a similar notice that also includes a specific description of the changes made to the privacy policies.

Security Provision/Requirements for breach of security:

- The bill requires providers to take reasonable security measures to protect customer proprietary information from unauthorized use, disclosure, or access.
- When a breach of the provider's security occurs, the provider is required to notify each affected customer within 30 days after learning of the breach unless the provider reasonably determines that no harm to the customer is reasonably likely to occur as a result.
- The notification must describe the information that is reasonably believed to have been involved in the security breach and include information about how to contact the provider to inquire about the security breach and how to contact relevant government agencies.
- If the security breach creates a risk of financial harm, the notification must also include information about steps that the customer can take to guard against identity theft.
- The bill also requires a provider to notify the Department of Agriculture, Trade and Consumer Protection and the Department of Justice within seven business days of learning about a breach of security affecting 5,000 or more customers unless the provider reasonably determines that no harm to customers is reasonably likely to occur as a result of the breach.

- If a breach of security affects fewer than 5,000 customers, the bill requires a provider to notify DATCP within 30 days after learning about the breach.
- Under the bill, a provider is required to maintain records for two years that contain information about the notifications made to customers about a breach of security.

Penalty

- A broadband Internet access service provider that violates the bill is subject to a civil forfeiture of up to $50,000 for the first violation, and up to $100,000 for each subsequent violation.
- Additionally, under the bill, any person or class of persons that is adversely affected by a violation by a broadband Internet access service provider can sue the provider for appropriate relief

Exceptions

- The bill allows the internet service provider to use a customer's proprietary information without receiving the customer's approval for the following purposes:
    - 1) to provide the broadband Internet access service from which the information is derived;
    - 2) to initiate, render, bill, or collect for broadband Internet access service;
    - 3) to protect the rights or property of a provider or to protect users against fraudulent, abusive, or unlawful use of the service;
    - 4) to provide certain services to a customer during a real-time interaction with the provider initiated by the customer;
    - 5) to provide location information or non-sensitive information in emergencies;
    - 6) or as otherwise required or authorized by law.

COUNCIL for CITIZENS AGAINST GOVERNMENT WASTE

February 14, 2018

Chairman Quinn, Members
Assembly Committee on Science and Technology

RE: Opposition to Assembly Bill 788

Dear Legislators,

On behalf of the 38,731 members of Council for Citizens Against Government Waste (CCAGW) in Wisconsin, I urge you to reject Assembly Bill 788. This proposed legislation would create instability and uncertainty for internet service providers (ISPs) and result in wasted tax dollars.

The internet is not contained within a single state's boundaries and therefore the participants in the internet ecosystem, including ISPs, can be regulated only by the federal government under the Commerce Clause, Article I, Section 8 of the Constitution. On December 14, 2017, the Federal Communications Commission (FCC) adopted the Restoring Internet Freedom Order, which restored the internet's proper classification as an information service, as was intended in the 1996 Telecommunications Act. It was under this light-touch regulation that the internet thrived and became one of the greatest innovations in history, as well as creating millions of high-paying jobs.

The FCC order also reinstated the Federal Trade Commission's (FTC) ability to investigate privacy and consumer protection violations by ISPs, and strengthens its enforcement capabilities by enhancing transparency requirements. Any ISP infringing upon consumer privacy or engaging in otherwise unfair conduct can be held accountable for its actions.

Efforts to undermine the FCC's order and usurp the FTC's authority, like Assembly Bill 788, would result in 50 different regulatory schemes for the internet, which would be impossible to navigate. There is little doubt that such a bill is preempted by federal law, and that taxpayer funds would be completely wasted footing the bill for a certain loss in federal court.

Broadband providers and consumers need predictability and stability on the internet, not a maze of rules and regulations. Assembly Bill 788 is both costly and unnecessary. It should be rejected.

Sincerely,

Thomas A. Schatz