



SHANNON ZIMMERMAN

STATE REPRESENTATIVE • 30th ASSEMBLY DISTRICT



Good Morning Chairman Quinn and Committee Members,

I first want to give a big thank you to Chairman Quinn and his office for facilitating such a speedy public hearing on this important issue. As many of you may know, I am a lifelong entrepreneur, with over two decades in the technology sector. Data privacy is something I have long cared about, so I appreciate everyone taking the time today to learn about this.

One of the advantages of my work has been to give me access to some of the greatest minds in the technology sector, many right here in Wisconsin. Based on those conversations, I have come to the conclusion we are about to enter a hyperinnovation phase as the result of three things converging: 1) big data, 2) artificial intelligence, and 3) quantum computing.

Big data is our increasing ability to extract useful conclusions from huge datasets, artificial intelligence is computers thinking for themselves, and quantum computing is using cutting edge physics to make computers with computational power unimaginable even a few years ago. These three innovations, if realized, would each individually fundamentally reshape our society, and bring enormous benefits in medicine, commerce, manufacturing, agriculture, and everything else. Put all three together, and the benefits are limitless.

But so are the risks. Technology companies are expecting to collect more data in the year 2020 than in every other year of previous human history, combined! And while data collection has already helped us in enormous ways, we have seen numerous abuses. Some examples:

- The New York Times published an article entitled *One Nation, Tracked*, where their reporters saw just a tiny sample of millions of citizens who's every movement throughout the day was being tracked by their cell phones, collected by private companies, and sold without their knowledge.
- An app now exists which utilizes facial recognition technology to allow anyone to snap a picture of a stranger, and return a complete profile on that person such as name, address, affiliations, and more. This app has recently received 'cease and desist' letters from Youtube, Facebook, Google, and Twitter for scraping through the billions of images on their websites.
- A company knew a teenage girl was pregnant before her father did. Based on the data collected on her, the company suddenly started mailing advertisements to their house on new baby items.
- A common one from surveys completed at DataPrivacyWI.com, is people noticing that their phones will pick up snippets of their conversations and advertise based on that.

Now take all of these examples, and exponentially increase the power of computer and datasets, and you can see why this is a huge problem. Imagine if this huge collection of data was taken by a government actor (i.e. federal prosecutors are alleging that the Chinese military was behind the Equifax breach), what could they do with all this information? There is a huge potential for abuse.

However, it doesn't have to be this way.

The Wisconsin Data Privacy Act is groundbreaking legislation that allows consumers to say 'no more, my data is my property!' Based on the European General Data Protection Regulation (GDPR), we take a model that **has been working since 2018 across a continent**, with which many US companies are already complying, and one that many privacy advocates (such as the International Association of Privacy Professionals) **consider a gold standard for consumers**.

Adoption of these bills would not only make Wisconsin the most consumer-friendly state in our nation on data privacy, but would provide a model for others to take action. The three bills work separately, but were conceived of as an entire package working together. The bills are:

Assembly Bill 870: Allows you to request a report from companies on what data they have on you. You would be given the contact information of someone at the company to request this, and companies would be required to let you know anytime they acquire your data.

Assembly Bill 872: allows you to tell a company to stop using or selling your data. The bill requires the company to get affirmative, specific consent from people before using their information.

Assembly Bill 871: allows you to request a company delete the data they have on you.

Across the bills, personal data is anything that can be directly tied to you, the consumer, so while your credit card or email would count, anonymized data would not. Some other exclusions include:

- Governmental and law enforcement information (this shouldn't be a loophole for criminals to evade their records).
- Information that is already available to the public.
- Data journalists may be using for stories, or artists may be using for literary purposes.
- Information you use purely in your home (so your kids can't request deletion of their list of chores).
- The bills also exclude many bits of data covered already under federal law, as much of this information is already protected in very specific ways, such as HIPPA law.

Another strong point about these bills are the penalties. These penalties are adapted from the GDPR which, again, is already in effect for any US company doing business in Europe. The Attorney General is responsible for enforcing these provisions. The stiff penalties give the bills needed teeth, otherwise the practical effect would exclude major companies who could easily absorb the costs imposed of legislation being proposed elsewhere.

Because of the complexity and interplay between the bills, I have included a copy of our cosponsorship memo for further explanation.

I know this is an incredibly busy time, so thank you once again to everyone for taking the time to her this bill, and I would love to answer any questions you may have.





The below is from our cosponsorship memo and gives more details on the three bills (updated with bill numbers):

Common Provisions

The WDPA consists of three separate, but interrelated bills, Assembly Bills 870, 872, and 871. Due to this, many provisions are very similar across the bills. The specifics of each bill are found below, but the following is common to all three:

Same Definitions

Consumer: means any person in Wisconsin

Controller: the individual who is responsible for the consumer's data. The definition **excludes** law enforcement, and federal, state, and local government individuals

Personal data: any information relating directly to the consumer, but excludes publicly available information

Process: anything done with data, including to sell, organize, alter, combine, publish, or otherwise

What the Bills DO NOT Apply To

The three bills exempt much of the same information, such as:

- Data collected for purely personal or household activity

- Information used for journalistic purposes
- Information used for literary or artistic purposes
- Information already covered by federal privacy laws, including in the areas of health, finances, patient safety work, credit reporting, driver information, and more.

Publicly available information is also excluded, as well as law enforcement or governmental information (at the federal, state, or local level).

Penalties

These penalties are adapted right from the GDPR which, again, is already in effect for any company doing business in Europe. In addition, only the Attorney General, an elected position, can enforce these provisions. The stiff penalties are needed to give the bills teeth, otherwise the practical effect would exclude major companies who can absorb the penalties as a cost of doing business.

Assembly Bill 870: Know Your Data

AB 870 allows a consumer (“individual”) to request reports explaining:

- **What** data a controller (“company”) is collecting on the individual;
- **When** the company is collecting it;
- **How** the company is using it
- **Who** the company is giving the personal data (“data”) to; and
- **How long** the company will retain the data.

This bill establishes a process for how **individuals can request their data**, including requiring companies to clearly publicize who an individual should contact and certain information associated with an individual’s data.

If the company did not originally collect the individual’s data, they must notify the individual they have it within one month of obtaining.

The report must be provided for free within one month (with a possible extension to three months) in electronic format, unless otherwise requested. If an individual’s request is manifestly unfounded or excessive (including by being repetitive), company may then charge a reasonable fee based on administrative costs, or refuse to act. The company bears burden of demonstrating that the request is unfounded.

Companies are not required to re-identify data (meaning to combine information together to identify someone) that does not identify the consumer, or retain data they wouldn’t otherwise retain.

Data Breaches

Companies are required to notify the Wisconsin Department of Justice (DOJ) within 30 days if they become aware of a data breach. If the breach is likely to result in a high risk to consumers, the company must notify the consumers whose personal data is involved in the breach, describing in clear and plain language nature of the breach. In limited circumstances, a company is not required to notify the DOJ or an individual, such as if steps are taken to mitigate the breach or the breach is unlikely to result in a risk to the rights and freedoms of individuals.

Penalties

Companies who intentionally violate the data breach requirements are subject to a fine of \$10,000,000 or up to 2 percent of total annual revenue, whichever is greater.

Companies who intentionally violate the bill's requirements related to providing copies of consumer's personal data, may be fined \$20,000,000, or up to 4 percent of total annual revenue, whichever is greater.

For additional details, please see the LRB Analysis and language, attached to this email.

Assembly Bill 872: Preventing the Sale and Use of Your Data

Under AB 872, an individuals must provide affirmative consent before a company can use their data, and allows individuals to request that companies stop use and sale of their data.

Authorization Required

Before a company can use an individual's data in any way, it must receive consent from the individual or the individual's guardian if the person is under 16 years old. Consent must be freely given, specific, informed, and unambiguous. **An individual can withdraw consent at any time.**

Individuals must be able to withdraw consent as easily as they give it, meaning companies can't simply make withdrawing consent overly difficult. Consent for data use must be clearly separate from other agreements (e.g. not part of a long and complex "User Agreement" page).

A company cannot require the collection and use of data as a condition for using their service, unless use of the individual's data is necessary for the use of the service.

Sensitive Data Categories Barred From Processing

AB 872 does not allow (with exceptions) companies to process the following specially protected categories of data:

- Racial, ethnic, political, religious or philosophical beliefs
- Genetic data concerning health, or information on sex life or orientation
- Biometric data (e.g. fingerprints), if used to uniquely identify the consumer

Controllers may process sensitive data for the following reasons:

- Processing is conducted for a purpose the consumer explicitly consents to;
- If it is necessary to comply with a legal obligation or required by legal proceedings or a court;
- The consumer is incapable of giving consent and processing is necessary to protect the vital interests of someone;
- Processing is conducted by a nonprofit having political, philosophical, or religious purposes of members' or those closely associated with the organization data, and the data **must not be disclosed outside the organization**.
- If the individual makes the data public;
- If the data is necessary for reasons of substantial public interest;
- If the data is needed to treat a medical emergency, or is necessary to protect against serious threats to public health or for ensuring the safety of medical products, it can be processed by a professional subject to governmental privacy laws;
- If processing necessary for historic or scientific purposes.

Request to Stop Processing

After receiving a request to stop processing, a company may not use an individual's data, with limited exception, but may continue to store an individual's data for limited, specific reasons.

A company is also required to notify every entity the company has shared data with to stop processing, unless notification is unreasonable.

Companies may still process data after a request to cease for the following reasons:

- Consumer re-consents to processing
- The data will be used for a legal claim
- To protect the rights of others
- For public interest reasons under state, federal, and local law

Data Usage Records

Under the bill, **companies are required to record the activities for which data is used**. The below is an example from the United Kingdom's Information Commissioner's Office ([see a written explanation here](#)):

Data usage records shall include:

- The company's name and contact information
 - Purpose of processing
 - Categories of data involved
 - Categories of individuals involved in processing
 - Documentation of consent
 - Name and contact information of who any data is disclosed to

A processor's (someone processing data on a company's behalf) records shall also include:

- The processor's name and contact information, along with the company information they are working on behalf of
 - Categories of processing conducted on behalf of each company

Processors must make these records available to DOJ on request.

Penalties

The attorney general may investigate violations of the bill.

Companies who intentionally violate the record keeping requirements are subject to a fine of \$10,000,000 or up to 2 percent of total annual revenue, whichever is greater.

Companies who intentionally violate the bill's requirements related to processing the consumer's personal data, may be fined \$20,000,000, or up to 4 percent of total annual revenue, whichever is greater.

For additional details, please see the LRB Analysis and language, attached to this email.

Assembly Bill 871: Delete Your Data

AB 871 requires companies to delete an individual's data if requested.

Deletion Request

Upon receiving a deletion request, a company shall delete the personal data relating to the consumer if any of the following applies:

- It is no longer necessary for the company to use the date for the purpose it was collected
- The data is used for direct marketing purposes
- The data has been illegally processed
- Deleting the data is necessary to comply with a legal obligation

The company shall also take reasonable steps to notify other entities they have shared data with that an individual has requested their data, and any links to the data, be deleted. Third parties are also required to delete the data. Deletion should occur within one month, but a company has up to three months to fulfill a deletion request if certain conditions are met.

Political, philosophical, or religious nonprofit organizations do not have to delete data if:

- They are only using the data on current or former members, or people who are closely associated with the organization; and/or
- The data will not be processed outside the organization

Penalties

The attorney general may investigate violations of the bill.

Companies who violate the bill's requirements related to deleting the consumer's personal data, may be fined \$20,000,000, or up to 4 percent of total annual revenue, whichever is greater.

A court may not impose the same action more than one fine on a controller unless the additional fine involves different activities.



State of Wisconsin
Governor Tony Evers

Department of Agriculture, Trade and Consumer Protection

Assembly Committee on Science and Technology AB 870, AB 871, and AB 872

Lara Sutherlin, Administrator, Division of Trade and Consumer Protection
Department of Agriculture, Trade and Consumer Protection
February 12, 2020

Chair Quinn and members of the Assembly Science and Technology Committee, thank you for the opportunity to testify for informational purposes only on the three bills that constitute the Wisconsin Data Privacy Act:

Wisconsin's Current Regulatory Framework

- Participating in today's digital economy means your personal identifying information is stored, shared, and sold like any other good or service. According to a November 2019 study by Credence Research, the data storage market is estimated to grow from \$56.8 billion in 2019 to \$144.3 billion by 2024.
- A 2019 report by the cybersecurity firm Risk Based Security indicates the total number of data breaches rose 33% in 2019 from 2018, with medical services, retailers and public entities most affected. The firm reported 5,183 data breaches that resulted in 7.9 billion exposed records.
- Wisconsin has a number of laws addressing the treatment of health, finance, and education data, to name a few. Wisconsin has only one law (Wis. Stat. § 134.98) that addresses the collection of consumer data, and it regulates only the notification required if there is a data breach. This law went into effect in 2006 and is deficient to address the challenges of data privacy and security posed by today's digital economy. The National Conference of State Legislatures (NCSL) did not identify any legislation in Wisconsin in any year between 2010 and 2019 in the realm of consumer data security or privacy. Given the dramatic changes in the marketplace, Wisconsin is well overdue for consideration of changes to its data privacy and security laws.

Comments About the Bills

DATCP commends the introduction of these bills and the legislative efforts to address the issues of data privacy and security. The bills are a promising first step in the right direction. DATCP would like to address generally some areas in the bills that should be refined.

- AB 870, (Wis. Stat. § 134.985 (4)), establishes a requirement to notify the Attorney General's office of data breaches without undue delay-- 30 days, if feasible. The three bills also establish an enforcement mechanism for the Attorney General's office to ensure compliance. Notification to and enforcement by a government entity is critical.

As the consumer protection agency for the State of Wisconsin, DATCP is charged with and has the allocated resources of law and staff to educate consumers, mediate complaints, and investigate violations of consumer protection law, be it a telemarketer or a home improvement company. DATCP regularly receives complaints about data breaches and identity theft. If DATCP is also notified of a breach, it could then better assist affected consumers in the aftermath of a data breach, including providing additional outreach where possible and identity theft assistance where necessary.

Wisconsin - America's Dairyland

2811 Agriculture Drive • PO Box 8911 • Madison, WI 53708-8911 • Wisconsin.gov

An equal opportunity employer

DATCP refers these investigations to the Attorney General or to District Attorneys for enforcement. Since data privacy and security fall squarely within DATCP's unfair business practices mandate, DATCP should not only be notified of breaches along with Attorney General but have the power to investigate and enforce violations of these laws.

In sum, if DATCP is notified at the onset and has the authority to enforce, it would expedite the best response to affected customers and use Wisconsin's best consumer resources. With DATCP's consumer hotline, mediation unit, and investigators, its resources better equip DATCP to address potential violations large and small.

- While AB 870 requires notification of the Attorney General within 30 days of becoming aware of the breach, the bill is less clear as to whether the notification must include the duration of the breach, if known to the "controller". To the extent that this may not be a requirement, DATCP believes it should.
- The bills preclude the ability for a district attorney to file charges. A data breach may be smaller or more localized and not rise to the standard that the Attorney General would take the case.
- The bills lack a private right of action for consumers as individuals. The Attorney General's office is the only permissible prosecutor. If an individual has a problem and the "controller," as defined by the bill, does not offer relief, a consumer has no other means of relief. As stated at the beginning of the testimony, the number of data breaches have increased at a precipitous clip. The Attorney General's office will not have the resources to take every case where just one or two consumers are denied deletion of files or do not provide consent. Allowing consumers to seek relief independently will better effectuate the intent of the law.
- The bills do not provide any rulemaking authority. Therefore, it leaves the statute without other guidance possible. Some of the language and terms are ambiguous. Under most circumstances, that may warrant rulemaking.
- The bills lack any requirement that businesses implement reasonable security measures. DATCP values prevention as consumer protection.
- The bills become law in two years. The data breach reporting provision in AB 870, after being amended to include DATCP, could go into effect sooner to protect consumers.

In conclusion, DATCP believes these bills are a positive step toward protecting consumers. They provide many needed rights and protections for consumers.

Thank you, Chair Quinn, for the opportunity to testify on these three bills. I will entertain any questions the committee may have.



WISCONSIN CABLE COMMUNICATIONS ASSOCIATION

22 East Mifflin Street, Suite 1010 • Madison, WI 53703 • 608/256-1683 • Fax: 608/256-6222

EXECUTIVE DIRECTOR - Thomas Moore

Statement of Tom Moore

Executive Director, Wisconsin Cable Communications Association

Before

Assembly Committee on Science and Technology

Speaking for Information regarding Assembly Bills 870, 871 and 872

Good morning, Chairman Quinn, and Committee Members. Thank you for the opportunity to appear today.

I am Tom Moore, Executive Director of the Wisconsin Cable Communication Association. We are the state trade association for Wisconsin cable video, broadband and voice providers. Our members provide voice, data and video service to roughly 900 Wisconsin communities and include household names like Charter Communications and Comcast as well as smaller regional and community systems like Lakeland Cable and Baldwin Telecom.

The cable industry values and relies on the trust and loyalty of its more than one million residential and business customers in Wisconsin. Our networks provide competitively priced high-speed broadband, video and voice services to neighborhoods of all types, from large cities to small towns and rural areas, from Fortune 100 customers to small businesses.

Ensuring that the privacy of our customers is protected is very important to us. And we appreciate the dialogue among policy makers, businesses, consumer groups and others about protecting privacy and security of consumers' personal information online.

We believe that consumer privacy is best addressed through the establishment of a national, federal framework, nevertheless, we look forward to continuing to work with the bill's authors, members of this committee and other stakeholders to provide input and expertise regarding this important policy matter.

Consumers Need a Comprehensive Online Privacy Framework

As you know, continuing advances in technology are changing the online privacy landscape. Despite Americans' daily reliance on websites, apps, and social media, it can be difficult for consumers to understand and appreciate how companies are collecting, analyzing, using and selling information about them.

An increasingly critical aspect of ensuring that consumers will continue to use our services and the multitude of offerings on the internet is making sure they have confidence that their online personal information is protected. While the cable industry strives to give our customers confidence with our current policies and practices, we recognize that there is still more to do.

The cable industry in the United States is taking a lead role in calling for a unified, comprehensive national privacy framework. It is our view that different policies that lead to inconsistent protections sow confusion and erode consumers' confidence in their interactions online. , For such a framework to be effective it must be applied consistently across the entire Internet ecosystem. From a consumer standpoint, they want their online data protected whether they are using an ISP, a search engine, an e-commerce site, a streaming service, a social network, or a mobile carrier or device.

A comprehensive privacy framework should seek to empower and inform consumers through rules that address five core principles – control, transparency, uniformity, parity and

security. We believe a federal solution would best accomplish these objectives by ensuring consumers are protected by a nationally consistent framework across the online ecosystem regardless of where they live or work.

We recognize that other states, not only Wisconsin, are seriously considering enacting their own state-level privacy regimes. As you consider legislation, we respectfully urge you to approach it from a similar place we do – based on the principles of transparency and consumer control. Such an approach enables consumers to decide how their data is used and at the same time allows companies to innovate.

Five Principles for Protecting Consumers Online

I would now like to address the five core principles that are critical to an effective privacy framework.

The first principle is control. Consumers should be empowered to have meaningful choice regarding the collection and use of their data. Any legal framework that is ultimately adopted should ensure consumer consent is purposeful, clear and meaningful. Additionally, consent should be renewed with reasonable frequency and any use of personal data should be reasonably limited to what the consumer understood at the time consent was provided. We recognize that there are several policy options which may be considered to allow consumers to exercise control over their data, and we are willing to work with stakeholders to find a common ground solution. Among those other ways are granting consumers the right to access and the right to delete their data, as proposed in the bills before this committee. We support those rights and look forward to working with the committee on developing a workable approach.

The second principle is transparency. Consumers should be given the information they need to provide informed consent. Explanations about how companies collect, use and maintain consumers' data should be clear, concise, easy-to-understand and readily available.

The third principle is parity. Consumers are best served by a uniform framework that is applied consistently across the entire internet ecosystem not based on who is collecting it, or what type of service is being offered. Consumer data should be protected equally whether they are using an ISP, a search engine, an e-commerce site, a streaming service, a social network, or a mobile carrier or device.

The fourth principle is uniformity. As I mentioned earlier in my testimony, for online consumer protections to be effective there should be a single national standard. A patchwork of state laws would be confusing for consumers, difficult for businesses to implement, and hinder continued innovation, yet, we realize that in the absence of a uniform, federal solution, some states may consider acting on their own. In doing so, it will be critical that the states understand what each of the others is doing so as to avoid an inconsistent or worse, contradictory, set of online protections.

The final principle is security. We believe privacy is security and security is privacy. Strong data security practices should include administrative, technical, and physical safeguards to protect against unauthorized access to personal data, and ensure that these safeguards keep pace with technological development.

Conclusion

Consumers today and in the future deserve to have the ability to control how their information is collected and used whenever they use the internet, and wherever they go online.

I thank the Members of the Committees for the opportunity to appear before you today on this important issue, and I would be happy to answer any questions you might have.

U.S. CHAMBER MODEL PRIVACY LEGISLATION



The U.S. Chamber's model privacy legislation would create a federal consumer privacy law that would eliminate a confusing patchwork of state laws. The model legislation draws upon the transparency, data sharing, and data deletion provisions of California's new consumer law, and data security elements of Europe's General Data Protection Regulation (GDPR).

The model legislation would:

- Eliminate a patchwork of regulations that would be confusing for consumers and businesses
- Empower consumers through transparency, opt-out, and data deletion
- Support innovation through regulatory certainty
- Task the Federal Trade Commission (FTC) with enforcement power

TRANSPARENCY AND CONSUMER CONTROL RIGHTS

Under the model legislation, businesses would take steps to proactively be clear and transparent about how a consumer's information is used. Businesses would be required to maintain and post a privacy policy that consumers can easily find. A business must also share how a specific consumer's personal information is being collected, used, and shared if requested by that consumer.

The model legislation includes consumer control rights. Through an opt-out provision, the model bill would give a consumer the ability to direct a business to stop sharing personal information with third parties. Under a data deletion provision, consumers would also have the right to request that businesses delete personal information.

SUPPORTING INNOVATION

Providing clarity to consumers and businesses about how data is used would support innovation and consumer confidence. The model legislation aims to create an environment where businesses know the rules of the road and consumers would be comfortable sharing personal information.

ENFORCEMENT

The FTC is tasked with enforcement of this model legislation. The bill empowers the FTC to require companies to offer and abide by consumer controls, including data deletion, opt-out rights, and transparency provisions. Companies that do not honor these controls would be in violation of the model bill and potentially subject to civil penalties. Currently, businesses are not required to offer these consumer controls.

Learn more at uschamber.com/data-privacy



U.S. CHAMBER OF COMMERCE



<https://www.uschamber.com/series/above-the-fold/we-need-federal-data-privacy-legislation>



U.S. Chamber of Commerce

We Need Federal Data Privacy Legislation

THOMAS J. DONOHUE

Chief Executive Officer, U.S. Chamber of Commerce

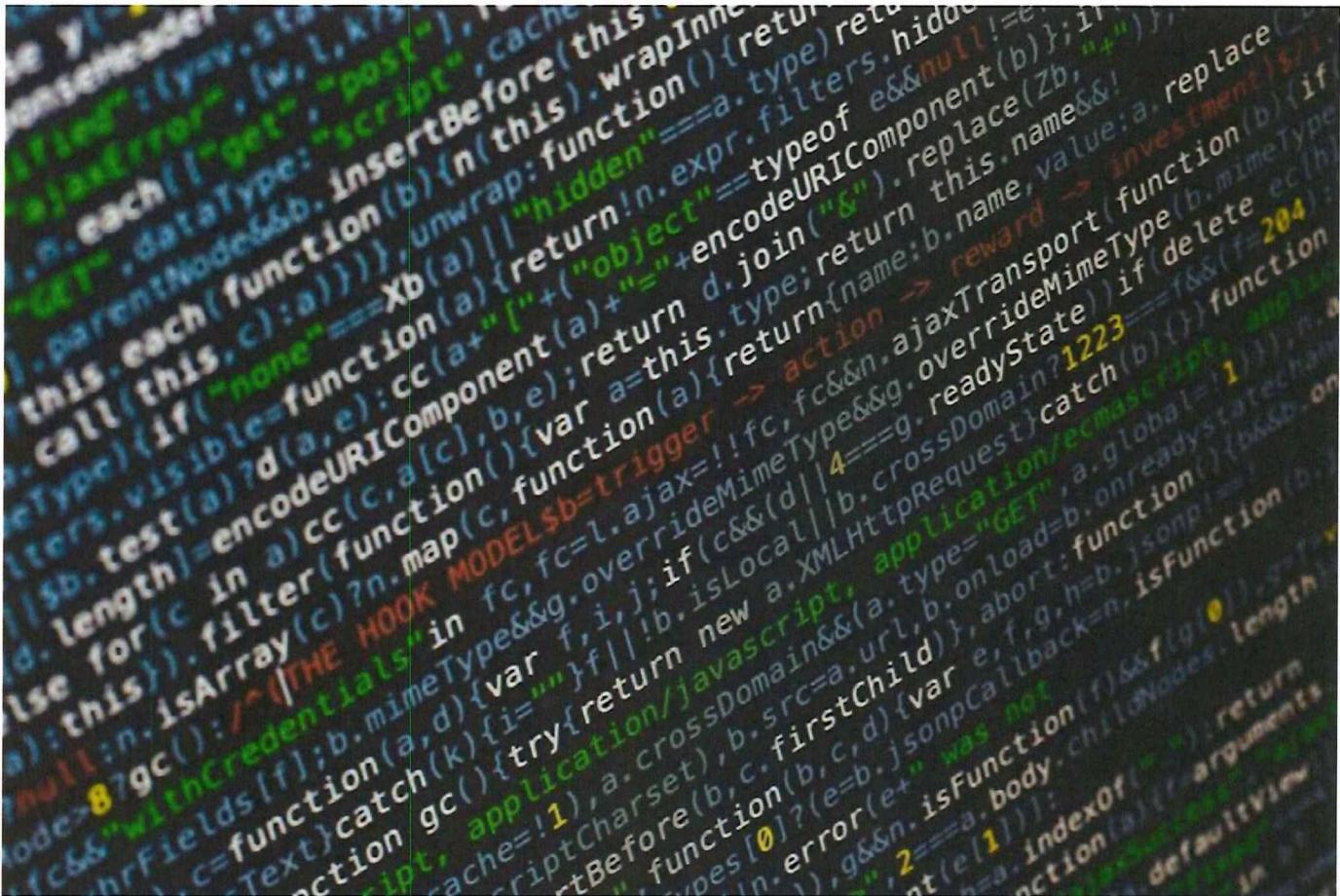


Photo by [Markus Spiske](#) on Unsplash.

Americans today enjoy more purchasing options, higher-quality products, and lower out-of-pocket costs than ever before. Our consumer-friendly marketplace has helped drive the last several years of economic growth, while improving the health and well-being of men and women across the country.

And what has made this possible? In a word, data.

Data-driven innovation is empowering Americans by expanding access to education and health care, as well as entrepreneurial and employment opportunities. It's helping small business owners streamline their operations, farmers increase their crop yields, and medical professionals save lives.

Data fuels our information economy and is an integral part of 21st century life. Smartphones are the perfect example. These devices have more computing power than the NASA rockets that sent a man to the moon. They are treasure troves of personal information that make our lives infinitely more convenient – but also more complicated and susceptible to risk. And it's the need to protect this personal information that has pushed the issue of data privacy to the fore.

Data privacy is a new frontier for regulation. In fact, all 50 states are racing to regulate how companies use data. To be sure, it's in everyone's interest to safeguard business and consumer data. But it must be done in a way that promotes innovation, provides regulatory certainty, and respects individual privacy and choice.

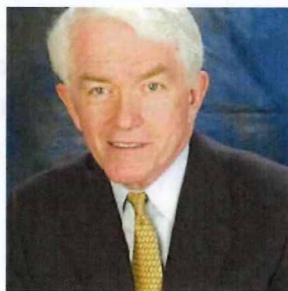
That's why earlier this month the U.S. Chamber of Commerce hosted Data Done Right, a national technology summit that convened business leaders from a cross-section of industries to build support for smart solutions, including the Chamber's draft data privacy legislation. Our proposal for a nationwide data privacy policy puts consumers first by allowing them to see and control how their personal information is being used.

It's not often that the Chamber asks for more regulation – much less writes it. But federal regulation in this arena is desperately needed to eliminate a patchwork of state privacy laws that would make interstate commerce and a seamless experience for Americans all but impossible. If we fail to act now on a national level, a flurry of conflicting state regulations will fill the void.

Also, creating a coherent and consistent privacy policy would preclude the lawsuit bonanza that would ensue without one. By establishing clear rules of the road, we can better protect individual privacy and avoid a 50-car pileup in the courtroom.

Responsible use of personal information is the linchpin of trust in today's tech-driven economy. That's why the Chamber will continue working to advance a national privacy framework to protect company and consumer data.

About the Author



Thomas J. Donohue

Chief Executive Officer, U.S. Chamber of Commerce

Thomas J. Donohue is chief executive officer of the U.S. Chamber of Commerce.

<https://www.uschamber.com/series/above-the-fold/establishing-clear-rules-of-the-road-data-privacy>

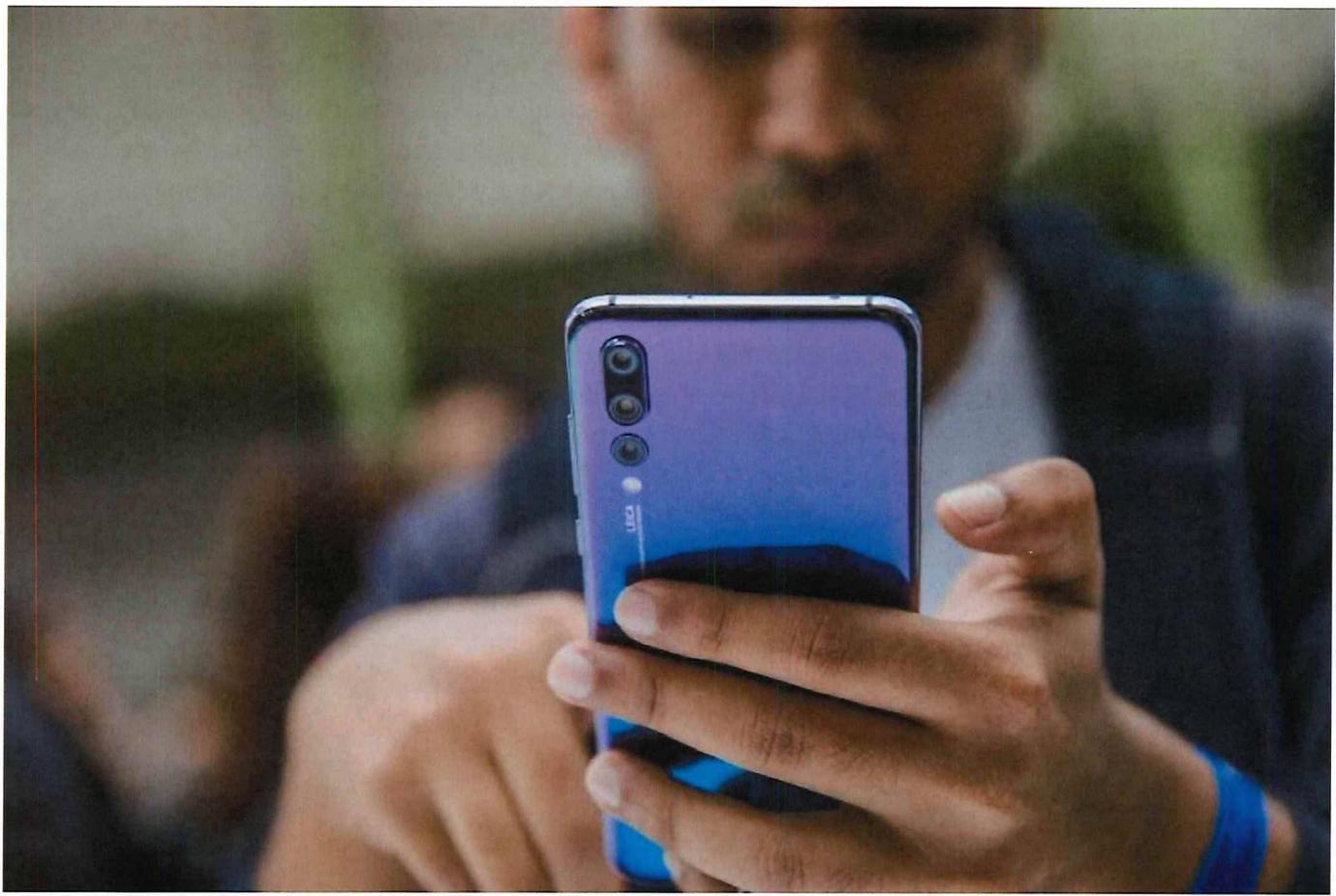


U.S. Chamber of Commerce

Establishing Clear Rules of the Road on Data Privacy

THOMAS J. DONOHUE

Chief Executive Officer, U.S. Chamber of Commerce



An attendee inspects a smartphone in Paris, France.

Photo credit: Marlene Awaad/Bloomberg

At the U.S. Chamber of Commerce, we believe it is possible to both protect individual privacy and promote technological innovation. That's why we unveiled model legislation this month that secures important new data privacy rights while providing businesses with the regulatory certainty they need to grow our economy and better serve consumers.

Data, when used responsibly, are invaluable to innovation, leading to new opportunities in education, entertainment, health care, and business creation. Likewise, data benefit consumers, who are able to take advantage of better services at lower costs. That's why it's in everyone's interest to protect data through smart policies that ensure regulatory clarity *and* individual privacy. To achieve both, the Chamber has taken the lead in drafting a privacy framework that provides clear and consistent guidelines.

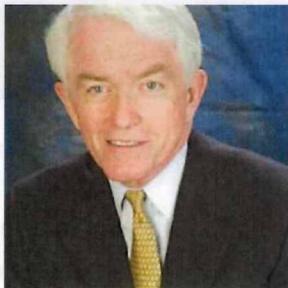
It's not every day that the Chamber asks for regulation. But data privacy is an important exception for two reasons. First, we believe that the responsible use of data is critical to business success. Second, we recognize that federal regulation in this arena is desperately needed to preempt a patchwork of state privacy laws that would make interstate commerce all but impossible. If we don't act now on a national level, then a flurry of conflicting state regulations will fill the void, causing headaches for companies and consumers alike.

That's why enacting a federal data privacy law is among our top priorities. Through our data privacy working group, we spearheaded a massive cross-industry effort to develop a proposal that puts everyone on the same page under one unifying federal framework. The logic is simple: It's far easier for businesses to operate under a single nationwide policy than having to navigate a labyrinth of idiosyncratic state privacy laws. Creating a coherent and consistent privacy policy would also preclude the lawsuit bonanza that would ensue without one. By establishing clear rules of the road, we can better protect individual privacy and avoid a 50-car pileup in the courtroom.

In addition to providing regulatory certainty, our proposal gives consumers important new rights. Specifically, it would allow consumers to see how their personal information is being used through easy-to-access privacy policies. It would also allow them to see how their information is being shared with outside parties. Consumers could even ask businesses to stop sharing their information or delete it altogether.

By striking the right balance between innovation and individual privacy, we can empower businesses to pioneer the next generation of life-changing technologies. For this reason, we urge lawmakers to carefully consider our model legislation.

About the Author



Thomas J. Donohue

Chief Executive Officer, U.S. Chamber of Commerce

Thomas J. Donohue is chief executive officer of the U.S. Chamber of Commerce.

ASSEMBLY COMMITTEE ON SCIENCE AND TECHNOLOGY

ASSEMBLY BILLS 870, 871, AND 872

TESTIMONY OF ZACHARY BEMIS ON BEHALF OF THE WISCONSIN INSURANCE ALLIANCE

February 12, 2020

Good Morning, Chairman Quinn and members of the Assembly Committee on Science and Technology.

We are testifying today on behalf of the Wisconsin Insurance Alliance (“WIA”). I’m Zach Bemis, a regulatory and administrative law attorney at Godfrey and Kahn, and former general counsel at the Wisconsin OCI. I am joined today by Justin Webb, the co-chair of our firm’s Data Privacy and Cybersecurity Practice Group in our Milwaukee office. Mr. Webb also serves as our firm’s Chief Information Security Officer and was the Information Security Officer at Marquette University, prior to entering private practice.

The WIA’s member companies are committed to protecting consumer privacy and data. We are speaking in opposition to the Wisconsin Data Privacy Act (“WDPA”) because we believe it takes the wrong approach for several reasons.

We hope to provide some important context and principles for the Committee to consider before it adopts the most onerous and economically stifling data privacy regime in the country. Those principles are: (1) avoid independent action, (2) use existing legal and regulatory structures, and (3) do not overreact.

These principles will ensure Wisconsin businesses and consumers are not placed at a competitive disadvantage when it comes to implementing data privacy protections. The Wisconsin Data Privacy Act fails to satisfy any of these principles.

The WIA represents insurance carriers of all sizes operating in Wisconsin. Some are already subject to the California Consumer Privacy Act, while others follow other insurance specific privacy statutes. All are part of the largest single industry in Wisconsin: the insurance industry.

Altogether, the industry contributes \$18.1 billion to the state’s GDP, and employs over 63,000 individuals, with an average industry salary of over \$71,000. Wisconsin is home to 332 domestic insurance companies (across all lines), fifth most of any state in the country.

It is worth pausing for a minute on the number of domestic companies and the scope of the insurance industry within Wisconsin. In part, our state attracts such a disproportionate number of insurance companies and insurance industry jobs because of the fair, efficient, and reliable regulatory climate this state has traditionally offered.

Avoid Independent Action

Our primary concern is that these proposals will upend Wisconsin's historical position and thriving insurance industry by creating millions of dollars in added compliance costs for potentially duplicative regulations without a clearly defined benefit.

Placing Wisconsin on a "regulatory island" increases the burden of doing business in the state and makes the state less attractive for all businesses, including insurance companies. Should the state proceed down this path, insurers – and all businesses – will be forced to examine the regulatory cost of doing business in this state.

California, through its size, and the European Union, through the concerted action of its member countries, were able to develop and compel compliance with their own data privacy frameworks. Wisconsin, is not able to compel compliance as California was able to do based on the size of its market. Independent action by Wisconsin, in contrast to the continent wide approach of the EU will also place Wisconsin at a competitive disadvantage.

Adopting European regulatory standards on insurance companies – and in fact all businesses in this state – would make Wisconsin an outlier within the United States. Should Wisconsin lead with the WDPA and no other states follow, the regulatory compliance paralysis created by the WDPA would greatly damage our insurance industry.

Use Existing Regulatory Structures

Wisconsin should not adopt sweeping legislation like WDPA without accounting for the unique regulatory nature of the insurance industry.

Data security and data privacy issues are top of mind for insurance companies and insurance regulators. Any action by Wisconsin in this arena should consider the existing regulatory framework rather than creating overlapping layers of regulatory red-tape. To summarize briefly:

- This committee today approved AB 819, a bill based on the National Association of Insurance Commissioners ("NAIC") Model Data Security Act, but customized to fit Wisconsin businesses. This legislation was developed through a deliberate process involving regulators, insurers, and consumer advocates, and relies on the OCI's regulatory authority.
- Insurance regulators take these issues seriously. Insurance companies undergo intensive examinations by state regulators. The NAIC Financial Examiner Handbook and the Market Regulation Handbook provide guidance on examining IT controls to help ensure entities are taking reasonable and necessary steps to protect consumers from theft or loss of personal information.
- The Privacy of Consumer Financial and Health Information Regulation, prompted by the Gramm-Leach-Bliley Act and adopted in Wisconsin's administrative code, already regulates nonpublic personal financial and health information. Among other things, that regulation requires insurers to (1) provide notice to consumers about its privacy policies

and practices; (2) describe conditions under which an insurer may disclose nonpublic information about individuals to affiliates and third parties, and (3) provide methods for individuals to prevent the disclosure of that information. Through the NAIC, state insurance regulators are currently considering whether revisions to this law are appropriate.

The fundamental concern with the WDPA is that it would place all insurance companies under an additional web of regulations, subjecting different types of data to different regulatory requirements with different state agencies.

Instead, the state should develop targeted regulations using existing regulatory structures. Any proposal affecting the insurance industry should be administered by the Office of the Commissioner of Insurance.

Don't Overreact

Data is often used for reasons that benefit consumer, in the form of product innovation, improved customer experiences, or lower rates. Some of this data falls within the scope of the vague and poorly defined definitions of the WDPA. Obstacles to the legitimate uses of data will greatly limit the development and delivery of these benefit to consumers.

Innovation is thriving in the insurance industry. Big data and predictive analytics are projected to make markets more competitive and consumer friendly. The Legislature must consider the benefits of these technologies alongside concerns for consumer privacy.

Data analytics have the potential to: (1) bring improvements to pricing and underwriting, ensuring risks are priced accordingly and maximizing societal benefits and optimal behavior, (2) increase customer satisfaction through better claim reporting and resolution, (3) improve coverages through the development of models involving dynamic simulations with variable losses, (4) mitigate fraud, and (5) increase operational efficiency within companies, further putting downward pressure on rates.¹

Conclusion

For these reasons, the WIA objects to the sweeping breadth of these proposals as they appear to apply to insurance companies. My colleague Justin Webb will now share experiences working with GDPR and CCPA and some additional critiques of the bill that we hope the authors and committee will consider.

Thank you.

21857673.3

¹ Big Data and Regulation in the Insurance Industry, Lawrence S. Powell, Ph.D, Executive Director, Alabama Center for Insurance Information and Research, available at:
https://www.naic.org/insurance_summit/documents/insurance_summit_2018_CIPR_01.pdf

ASSEMBLY COMMITTEE ON SCIENCE AND TECHNOLOGY

ASSEMBLY BILLS 870, 871, AND 872

TESTIMONY OF JUSTIN P. WEBB ON BEHALF OF THE WISCONSIN INSURANCE ALLIANCE

February 12, 2020

Mr. Chairman, members of the Committee, my name is Justin Webb. I am Co-Chair of the Data Privacy and Cybersecurity Practice Group with the Milwaukee office of Godfrey & Kahn, S.C, and I speak today on behalf of the Wisconsin Insurance Alliance (the “WIA”). Thank you for the opportunity to testify today.

To begin, we can all agree that privacy is a major concern for consumers, especially given the number of well-publicized data breaches and privacy mistakes of companies both large and small. There are a number of ways to approach the need for additional privacy protections for consumers and transparency from companies handling personal information. But, having reviewed Assembly Bills 870, 871, and 872 (together, the “Wisconsin Data Privacy Act” or the “WDPA”), the correct approach is not to directly import a Frankenstein-like mess of the most onerous requirements and exorbitant penalties from European privacy law to Wisconsin. There is a reason that even California did not elect to adopt something closely resembling the General Data Protection Regulation (the “GDPR”): the GDPR is the most onerous privacy law in the world.

We would urge the members of the Committee, and the Wisconsin legislature, to instead take a measured and incremental approach to privacy legislation, given the potential costs to and impacts on Wisconsin businesses. We think it is important to look to the expectations of U.S. consumers and address their main concerns, rather than looking to European laws and European consumer expectations, which are fundamentally different due to the differences in our economics, our rights, our laws, and our mores. Europe has had an over 25 year history of privacy regulation dating back to the Data Protection Directive in 1995. The WDPA, by contrast, attempts to cause a sea change in Wisconsin privacy law in just two years, and it would ensure that Wisconsin zooms toward over-regulation. This timeline is especially concerning for small businesses that have yet to be caught up in any comprehensive privacy regulations but would be under the WDPA.

The GDPR and the new California Consumer Privacy Act (the “CCPA”) have also become the *de facto* national standard, for better or for worse.¹ But, the WDPA does not attempt

¹ Kate Fazzini, *Europe’s Sweeping Privacy Rule Was Supposed to Change the Internet, But So Far It’s Mostly Created Frustrations For Users, Companies, and Regulators*, CNBC (May 5, 2019), available at <https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html>; Zack Whittaker, *California’s Privacy Law is Off to a Rocky Start*, TechCrunch (Feb. 8, 2020), available at <https://techcrunch.com/2020/02/08/ccpa-privacy-law-rocky-start/>.

to fall in line with U.S. privacy regulations or the CCPA, and instead cobbles together an entirely new standard, needlessly adding to the complex privacy landscape.

For example, the WDPA vastly restricts the processing of personal information and creates a permission-to-process-based system. This will inevitably stifle innovation at insurance companies, startups, and other technology-drive businesses living in an era of big data—innovation that is beneficial to consumers and creates tailored products and services. The CCPA does not restrict the processing of personal information in this way. The WDPA also requires Wisconsin businesses to notify consumers if they receive a consumer's personal information from another party, which would cause a massive influx of emails and written notices to consumers, subverting the privacy protection component of the law in favor of nuisance communications. The CCPA also has no such requirement. The WDPA also focuses heavily on consent as one of the sole bases for processing of personal information. But, obtaining consent from consumers can be incredibly difficult, especially when businesses collect personal information over the phone, in-person, and online in myriad ways. The consent requirements will needlessly inundate consumers with checkboxes, pop-ups, cookie consents, browser banners, and email opt-ins. The CCPA contains no consent requirements, except with respect to minors, and the CCPA also allows the processing of personal information if it is consistent with consumer expectations. The WDPA contains no such flexibility.

While the CCPA sounds less onerous than the WDPA, the rollout of the CCPA was also unimaginably flawed. There were last-minute amendments passed by the California legislature that materially changed the law. And, the California Attorney General has released three sets of differing regulations since the law's passage, including vastly different regulations released last Friday *after the law went into effect*. This legal chaos has caused mass confusion among businesses and complex compliance challenges for companies both big and small. In determining what privacy legislation is appropriate for Wisconsin, we would encourage you to understand and learn from the mistakes that have plagued the CCPA since its inception. It was a quickly-passed statute with little input from businesses, consumers, or other stakeholders.

One of those lessons to be learned from the CCPA is the massive cost it has and will have on California businesses. Consider that the initial compliance cost to businesses in California from CCPA is predicted to be \$55 billion² according to a study commissioned by the California Attorney General's Office and the California Department of Justice. The study also stated that compliance costs for the next decade could range from \$467 million to over \$16 billion. Most importantly, the study also found that the initial compliance cost to small businesses under 20 employees could be \$50,000, \$100,000 for companies up to 100 employees, \$450,000 for companies up to 500 employees, and \$2 million for companies over 500 employees.

² See Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, California Department of Justice by Berkeley Economic Advising and Research, LLC (August 2019), available at http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf; Lauren Feiner, *California's New Privacy Law Could Cost Companies a Total of \$55 Billion To Get In Compliance*, CNBC (Oct. 8, 2019), available at <https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html>.

Companies complying the CCPA are spending considerable amounts of money on attorney and consultant fees and thousands or tens of thousands of dollars on software products that handle data subject rights, cookies, and data mapping. You can imagine how much more it would cost Wisconsin businesses to comply with the WDPA. These costs will surely be passed on to consumers and lead to an increase in the price of products and services.

Having addressed the WDPA in the context of the CCPA and the GDPR at a macro level, we will next address the specific requirements and provisions of the WDPA. Among the concerning provisions in the bill:

- The WDPA proposes fines over \$20 million dollars, and the WDPA could be read to propose a *minimum* fine of \$10 million. The law also imposes fines on *data processors* that are determined by the revenue of *data controllers*. By comparison, the CCPA has fines of \$2500 for negligent violations and \$7500 for intentional violations, *and the CCPA includes a thirty (30) day period to cure for businesses*. To say that the penalties in WDPA are an outlier would be an understatement. The WDPA's exorbitant fines will likely (1) scare away foreign businesses from commerce with Wisconsin residents—similar to what occurred in 2018 when the GDPR caused U.S. businesses to withdraw from Europe,³ and (2) make new or existing businesses think twice about relocating to Wisconsin.
- The WDPA defines the term “personal data” in a manner that would include all sorts of rote personal information, including e-mail addresses. The WDPA also requires, unlike CCPA, that if a controller intends to process a consumer’s personal data and the controller did not receive it directly from the consumer, the controller must notify the consumer within thirty days. That means if a business person receives an incoming email from Sally that contains John’s business email address, say through a referral, the business person would be required to send an email to John and tell him all sorts of things. Wisconsin consumers would constantly receive emails telling them that their personal data had been shared, even if it was for wholly business purposes or for pro-business purposes—like a referral. And, the overhead necessary for businesses to comply with this requirement would be staggering.⁴ Indeed, the California legislature realized

³ Hannah Kuchler, *U.S. Small Businesses Drop EU customers over new data rule*, Financial Times (May 23, 2018), available at <https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04>. See also, Mike Masnick, *Companies Respond to The GDPR By Blocking All EU Users*, TechDirt (May 10, 2018), available at <https://www.techdirt.com/articles/20180509/14021739811/companies-respond-to-gdpr-blocking-all-eu-users.shtml>; Barbara Kollmeyer, *Chicago Tribune, Los Angeles Times Go Dark in Europe After GDPR Fail*, MarketWatch (May 25, 2018), available at <https://www.marketwatch.com/story/chicago-tribune-la-times-go-dark-in-europe-after-gdpr-fail-2018-05-25>; Renae Reints, *These Major U.S. News Sites are Blocked in the EU*, Fortune (Aug. 9, 2018), available at <https://fortune.com/2018/08/09/news-sites-blocked-gdpr/>.

⁴ Similarly, if an insurance agent was provided the name, email address, and telephone number of a prospect from a friend, the insurance agent would need to contact the prospect and provide a disclosure about how the insurance agent received that personal information, even if the prospect provided their information for that specific purpose. A final example is worthwhile. Finally, if an attorney received an email from a client that said company ABC wanted to fire Sally, under the WDPA the attorney would need to email Sally and let her know within thirty (30) days how the attorney obtained her information—that could be a problem if Sally doesn’t know she will be fired.

that regulating business contact information like names, email addresses, telephone numbers would be much too onerous. Indeed, the California legislature has currently stayed the CCPA's applicability to business-to-business personal information.

- The WDPA does not contain any exemptions for small businesses, or any other applicability or jurisdictional elements. The CCPA, on the other hand, exempts businesses that have less than \$25 million in revenue from the law entirely, subject to a couple of exceptions.⁵ And, the GDPR exempts businesses with fewer than 250 employees from the requirement to maintain records of processing activities, one of the more onerous requirements in the GDPR and the WDPA. The lack of exemptions is sure to place immense burdens on startups and small businesses, who do not have the resources to undertake data mapping, to implement cookie consent mechanisms, or to hire an attorney to assist them in their compliance efforts.
- The WDPA, unlike the GDPR, does not state that an entity's own marketing is a legitimate ground for processing personal information. This could significantly restrict the ability of responsible insurance companies and other businesses to market their products and services and interact with consumers, without a plethora of frustrating consent check-boxes, written and online notices, and signage. This will not enhance consumer privacy, but will instead train consumers to ignore those notices.
- The WDPA includes a plethora of undefined terms and, were that not enough, the law does not delegate the authority to issue regulations to the DOJ. Under the CCPA, the California Attorney General is tasked with drafting regulations and interpreting the law. In the EU, the European Data Protection Board is tasked with interpreting the law. Without an interpretive body, terms and phrases in the WDPA like "legitimate grounds" and "risk to the rights and freedom of consumers" will remain undefined. Are Wisconsin businesses supposed to look to European regulators to determine what those terms (or similar terms) mean? If the Wisconsin DOJ is the interpreter and enforcer of this law, does the DOJ have the manpower to do so?
- The WDPA confusingly exempts certain types of *information* from the law, as opposed to *entities*, and only exempts certain personal information from certain requirements. So, layering the WDPA on top of existing regulations would dramatically increase the compliance costs for insurance companies and other highly regulated entities. A more reasoned approach would be to completely exempt entities subject to federal comprehensive regulatory schemes like the Gramm-Leach-Bliley Act and its state counterparts, just as Wisconsin's current state data breach notification law does. The WDPA also does not exempt insurance companies or other highly regulated entities from the data breach reporting obligations. So, highly regulated entities would be subject to multiple different notice requirements in Wisconsin with different timing and content.

⁵ Entities under \$25 Million can also be subject to the CCPA in other scenarios, including where they collect the personal information of over 50,000 California residents, households, or devices. But, the point remains that the CCPA has applicability thresholds, and these laws do not.

- The WDPA requires insurance companies and other entities to maintain records of processing activities. But, it is nearly impossible for any organization to document exactly how they process personal information in e-mails, on telephone calls, and in their in-person interactions, without hiring teams of people to do so. Most organizations subject to the GDPR still have not properly met this requirement. And, asking companies to maintain records of what personal information is processed does not enhance consumer privacy. Rather, it is a costly paper pushing exercise.
- The WDPA contains a requirement to notify regulators and individuals of a “personal data breach,” which includes, among other things, accidental loss or alteration of personal data. Given that personal data includes all email addresses, telephone numbers, and other rote personal information, the DOJ will likely be deluged with breach notifications. Something very similar happened to EU regulators post-GDPR (and it continues).⁶ True, the WDPA states no notice is required to the DOJ if the personal data breach is “unlikely to result in a risk to the rights and freedoms of consumers,” but who knows what that means in the WDPA, and GDPR also said the same thing. This over-notification will slow down enforcement of truly important data breaches. Wisconsin’s existing data breach notification law, conversely, takes a reasoned position—requiring notification only for sensitive personal information. Even the California legislature elected to maintain a more restrictive definition of personal information in the CCPA to avoid this over notification problem. Consumers want notification when their sensitive personal information like credit card numbers, Social Security number, and biometric information are compromised, not when trivial incidents occur that have no practical effect on their privacy.
- The WDPA permits controllers to process sensitive personal information, like racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic data, and information about a consumer’s sex life or sexual orientation, if that information is made public. But, the WDPA *does not* permit a controller to process personal data that is not sensitive, like email addresses and phone numbers, if *that* information is made public. This, of course, makes absolutely no sense, and flips consumer expectations on their head. Most consumers expect that if they post personal information publicly, like their email address or contact information, that information is fair game for entities to process. Indeed, in some cases, individuals post their email address because they want to be contacted. And, businesses process publicly posted information to generate leads to sell their services to consumers, to contact attorneys, consultants, insurance agents, and many other professionals. Restricting the processing of information consumers and other have intentionally made public treats consumers like they do not understand the internet or privacy.

What all of this demonstrates is that privacy law is complex, and any privacy regulatory scheme must weigh the rights of consumers against the needs of businesses that process personal data for myriad reasons, most of which are not nefarious or harmful to consumer expectations. In highly

⁶ See Fazzini, *infra* at note 1.

regulated industries such as insurance, any potential regulations must also work within the existing regulatory structure.

Unfortunately, the WDPA does not adequately strike that balance. Taking a scalpel to European privacy law and attempting to transplant it into the complex web of federal and state laws in Wisconsin is doomed to make Wisconsin sicker instead of curing the state's perceived privacy ailments.

There is no doubt that the evolution of technology has given rise to legitimate privacy concerns for all individuals, and the legislature should eventually address this issue. But, we would urge the Committee to invest the time and careful thought necessary to address this ever-evolving issue in a way that does not scare businesses, stifle innovation, frustrate consumers, and add to the already large regulatory burden of Wisconsin insurance companies.

21854856.5



Wisconsin Council of Life Insurers

Parrett & O'Connell, LLP
10 East Doty St. – Suite 403, Madison, WI 53703
Phone: 608-225-4695

American Family Life Insurance Company
Catholic Financial Life
CUNA Mutual Insurance
MetLife
National Guardian Life Insurance Company
Northwestern Mutual
OneAmerica Financial
Prudential Life Insurance
State Farm Life Insurance Company
Thrivent Financial
WEA Trust

MEMORANDUM

TO: HONORABLE MEMBERS OF THE ASSEMBLY COMMITTEE ON SCIENCE AND TECHNOLOGY

FROM: CONNIE O'CONNELL

DATE: FEBRUARY 12, 2020

SUBJECT: ASSEMBLY BILLS 870, 871 and 872 RELATING TO CONSUMER DATA

The Wisconsin Council of Life Insurers (WCLI), an organization representing both domestic and nondomestic life insurance companies licensed in Wisconsin, appreciates the opportunity to raise concerns with Assembly Bills 870, 871 and 872 relating to consumer access to data, deletion of data and restrictions on use of data.

The insurance industry has long been a leader in protecting consumer data and supporting clear obligations in the appropriate collection, use and sharing of sensitive personal information. In fact, one week ago today, WCLI appeared before this committee to support Assembly Bill 819 creating additional protections under Wisconsin law to ensure the security of consumer data. Our support of AB 819 is consistent with the role of our industry in establishing a comprehensive and consistent federal and state regulatory framework governing the use and disclosure of personal information by the insurance industry. This framework, which includes the Gramm Leach Bliley Act, Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act Privacy Rule, Wisconsin statutes regulating the disclosure of personal medical information, § 610.70, Wis. Stat. and Chapter Ins 25 Privacy of Consumer and Financial Health Information is tailored to the insurance and financial services sector, providing strict standards for the unique types of information collected by insurers and appropriate use of the data to conduct necessary underwriting, pricing, claims management and fraud prevention activities. In addition, the system provides for accountability within the insurance regulatory framework.

Because of the existing structure of state and federal data privacy and security laws applicable to insurers, superimposing the proposed package of bills over the current obligations will result in conflicting and unclear requirements, restraints on necessary insurance functions and significant implementation costs. Consumers will also likely struggle with understanding what their rights are and how their information is protected when dealing with the proposed multilayered complex regulations.

WCLI respectfully requests the committee not support Assembly Bills 870, 871 and 872.



Assembly Committee on Science and Technology

2019 Assembly Bills 870, 871, and 872

Consumer Personal Data Privacy

February 12, 2020

Good morning Chairman Quinn and members of the Assembly Committee on Science and Technology. Thank you for the opportunity to provide written testimony on behalf of the University of Wisconsin-Madison for informational purposes on Assembly Bills 870, 871, and 872 (AB 870, AB 871, AB 872), which relate to the access, use, and deletion of consumer personal data.

The University of Wisconsin- Madison and its sister institutions within the state heavily depend upon personal data either directly collected or collected by other non-profit agencies with the intention of identifying prospective students. Our understanding of this legislation is that the University of Wisconsin System, including UW-Madison, is a unit of the state government and thus is not considered a “controller” or “processor.” We are grateful to Representative Zimmerman and the other representatives who introduced and co-sponsored this bill for the thoughtfulness and consideration of such a necessary and appropriate exemption for our public colleges and universities.

Yet, we are concerned that other educational non-profit agencies whose services are critical to the college-readiness process may not be exempted under these bills. Organizations who perform standardized testing, college preparatory services like the ACT and the CollegeBoard, that administers both Advanced Placement (AP®) and the SAT ® as well as other institutions that serve students in our state and local communities like the 4-H, Future Farmers of America, the Wisconsin Rural Schools Alliance (WiRSA), the Boys & Girls Club and the Goodman Community Center will collect basic personal data from time-to-time on their student participants for a variety of reasons and with varying degrees of technological sophistication and resources.

Under Assembly Bills 870, 871, and 872, these organizations would be acting as “controller” and/or “processor” when collecting data on students for purposes of local scholarship applications, camp and service participation, nomination and recommendations to colleges, universities and other education-related programs. These organizations whose resources are intended for the public

good and service would have to make serious technological, human and professional resource investments that their budget structure simply does not support and would be detrimental in their continuing service to students and families across our state.

Assembly Bill 872 also provides that consumers under the age of 16 are required to have parent or guardian consent by, "...a statement or clear affirmative action". We believe that the protection of minors and other vulnerable parties is serious and applaud this bill and its design to protect those who could not otherwise provide informed consent against those with malintent and simply seeking profits.

Under this bill, organizations seeking to directly serve those students would be limited in their ability to meet the needs of our most vulnerable citizens in all corners of our state. We therefore respectfully request that an exemption for non-profit educational organizations be provided in this legislation to enable the continued collection of data to serve students, many of whom in the most impoverished parts of our state may not have parents or guardians who are able to be active in their college-going process.

The University of Wisconsin-Madison has been in contact with the bill author and appreciates the recognition of exemptions for public colleges and universities already provided and we hope our testimony provided a brief overview of some of the concerns we share with other organizations and citizens of Wisconsin. We look forward to continuing to work with the author, the Legislature, and members of this committee on this important issue and our feedback. On behalf of the UW-Madison we would like to thank you for your time. If you have any questions please reach out to Assistant Director of State Relations, Ben Van Pelt, at (815) 474-3973 or via at bmvanpelt@wisc.edu.



February 12, 2020

The Honorable Romaine Quinn

Chair, Committee on Science and Technology

Room 323 North

State Capitol

PO Box 8953

Madison, WI 53708

Dear Chairperson Quinn and Members of the Committee on Science and Technology:

On behalf of more than 90 businesses represented by CompTIA, the leading voice and advocate for the global information technology industry, we respectfully oppose Assembly Bills 870, 871, and 872 because of their excessive fines, lack of clarity/conflicting language, added compliance costs and the regulatory burdens created by these bills.

CompTIA is an advocate for consumer security and privacy. We support thoughtful policies that are workable to ensure that consumer data is secure, protected, and accessible. Language for Assembly Bills 870, 871, and 872 is confusing, and at times, conflicting. There is currently not an exemption for fraud in all three measures, enforcement is inconsistent, and language conflicts with recently enacted legislation in California that many of our members must comply with – itself fraught with confusion, unknown variables, and high implementation costs.

The potential financial constraints of these measures are also of significant concern for our membership. The 450,000 small businesses in the state represent over 99 percent of all businesses in Wisconsin, and they employ 1.2 million people, or 49.7 percent of the Wisconsin workforce (Wisconsin Small Business Administration). Measures such as this impact all businesses, but in particular small businesses. In California, where legislation has recently been enacted, the added cost to small businesses are projected to be \$50,000 for companies with less than 20 employees, and \$100,000 for companies with less than 50 employees. In whole, costs in California are estimated to be \$55 billion for initial implementation. This is just for one state, and one type of data privacy structure. As this committee meets, there are multiple bills under consideration across the country addressing some form of consumer data privacy. The consequences of additional state privacy standards would add to these costs, in addition to the excessive and potentially debilitating fines for violation in these measures.

Finally, enacting a new set of data privacy laws in the state of Wisconsin compounds the already burdensome regulatory environment our member companies must adhere to. Of those states considering their own data privacy laws, some are modeled after California's new – and untested – law. One measure in Illinois combines components of both California and a version of privacy legislation under consideration in Washington. Wisconsin Assembly Bills 870, 871, and 872 add the European Union's law on data protection and privacy, the General Data Protection Regulation (GDPR), into the mix. This is particularly problematic for businesses that are not equipped to comply with European law. Ideally, this issue should be addressed at the Federal level, where two pieces of

legislation are currently under consideration. This will ensure online security for all Americans without creating a myriad of conflicting state laws.

Thank you for your consideration and the opportunity to communicate the concerns of our membership regarding Assembly Bills 870, 871, and 872. We appreciate the sponsor's attention to this important issue, but respectfully oppose these bills and encourage the passage of privacy laws that protect consumer privacy without harming the state's economy or placing undue burden on business.

Respectfully,

Elizabeth Moe Garcia
Director of State Government Affairs- Midwest Region
CompTIA
3500 Lacey Road #100
Downers Grove, IL 60515

STATE PRIVACY AND SECURITY COALITION

February 12, 2020

Representative Romaine Quinn
Chairman, Assembly Committee on Science and Technology
Room 323 North
State Capitol
PO Box 8953
Madison, WI 53708

Re: Assembly Bills 870, 871, and 872

Mr. Chairman and Members of the Committee,

The State Privacy and Security Coalition, a coalition of 29 leading technology, retail, payment card, online security, automobile, and communications companies, as well as 8 trade associations, writes to comment on Assembly Bills 870, 871, and 872, concerning consumer data privacy.

Our coalition strongly supports the passage of federal privacy legislation to ensure that all US consumers have the same control, rights, and transparency regardless of their location. Until that outcome becomes more likely, we understand that states will consider ways to best provide their own residents with strong privacy protections. Given this session's calendar, Wisconsin has the luxury of time to carefully study and consider the potential consumers and business impacts of state privacy legislation.

To that end, we offer the following principles that we believe can help Wisconsin avoid many of the mistakes other states have made when drafting privacy legislation. Consumers and businesses alike are best served when legislation balances increased consumer control and transparency, operational workability, and cybersecurity. Our coalition thinks the following principles drive a solution that appropriately achieves this complex balance, and would be happy to work with the legislature and other stakeholders to get it right.

1. Definitions Matter

Particularly in consumer privacy legislation, definitions are critical to the ultimate success of the legislation. A workable set of definitions sets the scope of the bill and avoids unnecessary ambiguities that increase both consumer confusion and an entity's compliance costs. As an example, we believe that a proper definition of "Personal Information" should not list every possible descriptor of what personal information might be. This is unsustainable over time as new technologies emerge, and increases the chances that each legislative session, multiple bills will be filed seeking to clarify, expand, or narrow these elements.

Instead, a definition of Personal Information should provide flexibility over time, describing the nexus between the information and its ability to identify an individual in a way that is

STATE PRIVACY AND SECURITY COALITION

meaningful for both consumers and companies that store this data. Additionally, it should encourage and incentivize the use of de-identified data, which increases consumer privacy.

Likewise, a clear definition of “Sale” benefits consumers and businesses alike. Consumers are able to understand what a “sale” of data is, and thus are able to more clearly distinguish between entities that are selling their data vs. those that aren’t; businesses can avoid being negatively labeled for normal business-to-business transactions that, under the California Consumer Privacy Act’s (CCPA) overly expansive definition, trigger “do not sell my information” requirements, such as using free website analytics tools. In order to cover transfers of data that are non-monetary in nature, a clear definition of “disclose” can be used.

Finally, clear definitions avoid (or minimize) unintended consequences. In CCPA for instance, the threshold for applicability to a business is based partly on having greater than \$25 million in revenue. But it does not specify whether this means in-state, nationally, or globally. It is one of the most frequently asked questions by companies attempting to understand and comply in good faith, but there is no clarity – and such clarity is unlikely to be provided before the law goes into effect.

2. Core Consumer Rights Should Be Included But Carefully Drafted

We support the inclusion of core consumer rights, including the right to access, deletion, and opting out of sale. For reasons of operational workability, we do not believe that the inclusion of a GDPR-style “right to object” or “right to restrict processing” are appropriate rights for states to impose. Additionally, neither the CCPA nor the Washington Privacy Act (which is heavily based on GDPR) contains these rights. In order to avoid a patchwork of inconsistent state laws, we urge you to bear in mind the requirements promulgated in other states and ensure that for the significant number of companies who operate nationally, there are not conflicting or additional rights that would further confuse consumers.

3. Incentivizing Pro-Privacy Behavior, Rather Than Prohibiting Types of Processing, is a More Holistic and Realistic Regulatory Approach

We would encourage members of this committee to adopt an approach to privacy regulation that incentivizes pro-privacy behavior, rather than outright prohibitions on processing, or adopting a largely opt-in consent framework that contravenes the realities of the online ecosystem.

In addition to providing consumer rights, there are ways to accomplish this aim. Recognizing that there are core operational processes that consumers expect businesses to undertake for everyday activities (such as processing and fulfilling orders, first party marketing, and ensuring network functionality), instituting stricter controls over sensitive information (such as precise geolocation information) can provide consumers with important context to help them make decisions. This type of framework also allows businesses to evaluate whether they want to accept the high scrutiny that comes with processing this type of information.

STATE PRIVACY AND SECURITY COALITION

As a corollary, exempting information that is not linked or linkable to an individual from regulatory requirements is a positive incentive that both protects consumers' data and reduces compliance costs for businesses.

4. The CCPA is not a viable model

We appreciate that these bills do not propose to adopt the CCPA. However, as we anticipate that discussion of the CCPA will be a part of any conversation about state privacy legislation, we think it is important to describe the current state of that law.

Although part of the statute went into effect January 1, there are still significant changes likely to be implemented. First, the Attorney General's regulations are scheduled to be released sometime in the second quarter of 2020, with implementation beginning July 1, 2020. The initial draft was twenty-five pages of additional substantive requirements. The latest draft – released just last Friday – modified those requirements further, adding new requirements and deleting others.

Second, the original drafter of the 2017 CCPA ballot initiative has decided that he was unsatisfied with the ultimate outcome of CCPA, and consequently is gathering signatures to put forth another ballot initiative for 2020. This will significantly overhaul the current text of the statute, and create new, additional requirements.

Since its passage in June 2018, and including the two vehicles referenced above, the CCPA will have been amended *eight times* in just over two years. This is not the kind of sustainable, long-term vision that a state should apply to privacy law that governs cutting edge technology. Finally, CCPA is incredibly and needlessly costly to the business community. The Attorney General's own study estimated that the cost of *initial* compliance costs for implementation would total \$55 billion. For businesses with 20 or fewer employees, costs are estimated at \$50,000. For businesses with fewer than 50 employees, costs are estimated at \$100,000.

The CCPA's core aims – to provide consumers more transparency and control – can be accomplished with much simpler, much more comprehensible language that increases consumer benefit while reducing implementation costs. For these reasons, our coalition appreciates Wisconsin's willingness to consider alternatives.

5. Attorney General Enforcement is the Proper Enforcement Mechanism

We also appreciate that the bills before this committee propose enforcement through the state Attorney General.

No state – including California – has passed consumer privacy legislation that includes a private right of action for the privacy-related provisions. That is because the privacy requirements instituted by such legislation are very operationally and technically complex, and turning enforcement over to the trial bar presents very real threats without providing the same consumer benefits.

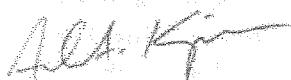
STATE PRIVACY AND SECURITY COALITION

Instead, we favor enforcement by the Attorney General as proposed in these bills (although we believe the penalty structure needs further discussion). The Attorney General is not motivated by external factors such as the leverage of high eDiscovery costs that lead to a settlement (enriching only the plaintiffs' attorneys), but is instead charged with enforcing the public interest and punishing bad actors. It has the expertise to be thoughtful and careful arbiters of entities' privacy practices while at the same time seeking to clarify, rather than exploit, any statutory ambiguities. This helps avoid uncertainties being resolved through litigation and also helps responsible actors know how best to comply.

Legislation along these lines is technical and complex. We believe that a careful and inclusive stakeholder process is critical to providing both meaningful consumer protection and also operational workability.

We would be happy to discuss these issues further and look forward to a productive dialogue.

Respectfully submitted,



Andrew A. Kingman
General Counsel
State Privacy & Security Coalition

STATE PRIVACY AND SECURITY COALITION

February 12, 2020

Representative Romaine Quinn
Chairman, Assembly Committee on Science and Technology
Room 323 North
State Capitol
PO Box 8953
Madison, WI 53708

Re: Assembly Bills 870, 871, and 872

Mr. Chairman and Members of the Committee,

The State Privacy and Security Coalition, a coalition of 29 leading technology, retail, payment card, online security, automobile, and communications companies, as well as 8 trade associations, writes to comment on Assembly Bills 870, 871, and 872, concerning consumer data privacy.

Our coalition strongly supports the passage of federal privacy legislation to ensure that all US consumers have the same control, rights, and transparency regardless of their location. Until that outcome becomes more likely, we understand that states will consider ways to best provide their own residents with strong privacy protections. Given this session's calendar, Wisconsin has the luxury of time to carefully study and consider the potential consumers and business impacts of state privacy legislation.

To that end, we offer the following principles that we believe can help Wisconsin avoid many of the mistakes other states have made when drafting privacy legislation. Consumers and businesses alike are best served when legislation balances increased consumer control and transparency, operational workability, and cybersecurity. Our coalition thinks the following principles drive a solution that appropriately achieves this complex balance, and would be happy to work with the legislature and other stakeholders to get it right.

1. Definitions Matter

Particularly in consumer privacy legislation, definitions are critical to the ultimate success of the legislation. A workable set of definitions sets the scope of the bill and avoids unnecessary ambiguities that increase both consumer confusion and an entity's compliance costs. As an example, we believe that a proper definition of "Personal Information" should not list every possible descriptor of what personal information might be. This is unsustainable over time as new technologies emerge, and increases the chances that each legislative session, multiple bills will be filed seeking to clarify, expand, or narrow these elements.

Instead, a definition of Personal Information should provide flexibility over time, describing the nexus between the information and its ability to identify an individual in a way that is

STATE PRIVACY AND SECURITY COALITION

meaningful for both consumers and companies that store this data. Additionally, it should encourage and incentivize the use of de-identified data, which increases consumer privacy.

Likewise, a clear definition of “Sale” benefits consumers and businesses alike. Consumers are able to understand what a “sale” of data is, and thus are able to more clearly distinguish between entities that are selling their data vs. those that aren’t; businesses can avoid being negatively labeled for normal business-to-business transactions that, under the California Consumer Privacy Act’s (CCPA) overly expansive definition, trigger “do not sell my information” requirements, such as using free website analytics tools. In order to cover transfers of data that are non-monetary in nature, a clear definition of “disclose” can be used.

Finally, clear definitions avoid (or minimize) unintended consequences. In CCPA for instance, the threshold for applicability to a business is based partly on having greater than \$25 million in revenue. But it does not specify whether this means in-state, nationally, or globally. It is one of the most frequently asked questions by companies attempting to understand and comply in good faith, but there is no clarity – and such clarity is unlikely to be provided before the law goes into effect.

2. Core Consumer Rights Should Be Included But Carefully Drafted

We support the inclusion of core consumer rights, including the right to access, deletion, and opting out of sale. For reasons of operational workability, we do not believe that the inclusion of a GDPR-style “right to object” or “right to restrict processing” are appropriate rights for states to impose. Additionally, neither the CCPA nor the Washington Privacy Act (which is heavily based on GDPR) contains these rights. In order to avoid a patchwork of inconsistent state laws, we urge you to bear in mind the requirements promulgated in other states and ensure that for the significant number of companies who operate nationally, there are not conflicting or additional rights that would further confuse consumers.

3. Incentivizing Pro-Privacy Behavior, Rather Than Prohibiting Types of Processing, is a More Holistic and Realistic Regulatory Approach

We would encourage members of this committee to adopt an approach to privacy regulation that incentivizes pro-privacy behavior, rather than outright prohibitions on processing, or adopting a largely opt-in consent framework that contravenes the realities of the online ecosystem.

In addition to providing consumer rights, there are ways to accomplish this aim. Recognizing that there are core operational processes that consumers expect businesses to undertake for everyday activities (such as processing and fulfilling orders, first party marketing, and ensuring network functionality), instituting stricter controls over sensitive information (such as precise geolocation information) can provide consumers with important context to help them make decisions. This type of framework also allows businesses to evaluate whether they want to accept the high scrutiny that comes with processing this type of information.

STATE PRIVACY AND SECURITY COALITION

As a corollary, exempting information that is not linked or linkable to an individual from regulatory requirements is a positive incentive that both protects consumers' data and reduces compliance costs for businesses.

4. The CCPA is not a viable model

We appreciate that these bills do not propose to adopt the CCPA. However, as we anticipate that discussion of the CCPA will be a part of any conversation about state privacy legislation, we think it is important to describe the current state of that law.

Although part of the statute went into effect January 1, there are still significant changes likely to be implemented. First, the Attorney General's regulations are scheduled to be released sometime in the second quarter of 2020, with implementation beginning July 1, 2020. The initial draft was twenty-five pages of additional substantive requirements. The latest draft – released just last Friday – modified those requirements further, adding new requirements and deleting others.

Second, the original drafter of the 2017 CCPA ballot initiative has decided that he was unsatisfied with the ultimate outcome of CCPA, and consequently is gathering signatures to put forth another ballot initiative for 2020. This will significantly overhaul the current text of the statute, and create new, additional requirements.

Since its passage in June 2018, and including the two vehicles referenced above, the CCPA will have been amended *eight times* in just over two years. This is not the kind of sustainable, long-term vision that a state should apply to privacy law that governs cutting edge technology. Finally, CCPA is incredibly and needlessly costly to the business community. The Attorney General's own study estimated that the cost of *initial* compliance costs for implementation would total \$55 billion. For businesses with 20 or fewer employees, costs are estimated at \$50,000. For businesses with fewer than 50 employees, costs are estimated at \$100,000.

The CCPA's core aims – to provide consumers more transparency and control – can be accomplished with much simpler, much more comprehensible language that increases consumer benefit while reducing implementation costs. For these reasons, our coalition appreciates Wisconsin's willingness to consider alternatives.

5. Attorney General Enforcement is the Proper Enforcement Mechanism

We also appreciate that the bills before this committee propose enforcement through the state Attorney General.

No state – including California – has passed consumer privacy legislation that includes a private right of action for the privacy-related provisions. That is because the privacy requirements instituted by such legislation are very operationally and technically complex, and turning enforcement over to the trial bar presents very real threats without providing the same consumer benefits.

STATE PRIVACY AND SECURITY COALITION

Instead, we favor enforcement by the Attorney General as proposed in these bills (although we believe the penalty structure needs further discussion). The Attorney General is not motivated by external factors such as the leverage of high eDiscovery costs that lead to a settlement (enriching only the plaintiffs' attorneys), but is instead charged with enforcing the public interest and punishing bad actors. It has the expertise to be thoughtful and careful arbiters of entities' privacy practices while at the same time seeking to clarify, rather than exploit, any statutory ambiguities. This helps avoid uncertainties being resolved through litigation and also helps responsible actors know how best to comply.

Legislation along these lines is technical and complex. We believe that a careful and inclusive stakeholder process is critical to providing both meaningful consumer protection and also operational workability.

We would be happy to discuss these issues further and look forward to a productive dialogue.

Respectfully submitted,



Andrew A. Kingman
General Counsel
State Privacy & 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

February 11, 2020

WWW.CDIAONLINE.ORG

The Honorable Romaine Quinn
The Honorable Kevin Peterson
Assembly Committee on Science and Technology
411 State St, Madison, WI 53702

RE: Assembly Bills 870, 871, 872 Concerning Consumer Privacy

Dear Chairman Quinn and Vice Chairman Peterson:

I write on behalf of the Consumer Data Industry Association (CDIA) to express our opposition to Assembly Bills 870, 871, and 872, acts concerning consumer privacy. Although, each of these bills strive to create privacy legislation aimed at protecting consumers. As drafted, they have the potential to create significant unintended consequences that could undermine privacy and data security.

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.

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 CRAs. Consumers have the right to dispute the completeness or accuracy of information contained in their files. Once a consumer

notifies the CRA of the dispute the CRA must reinvestigate and record the current status of the disputed information, or delete it from the record. The CRA must also notify the furnisher of the disputed data of the consumer's dispute.

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.

An example of potential harm that could happen if one does not take into account the different sectors and the specific uses for that data is applying things, such as "the right to deletion" or the "right to review the information" of 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. 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. Of the three bills in this package on AB 871 provides an exemption for fraud prevention.

However, even when a comprehensive privacy bill recognizes that exemption language is necessary, for things such as fraud, FCRA, GLBA, and public records, getting those exemptions properly written matters. For example, the current FCRA exemption in these three bills is problematic as it is currently drafted and could potentially cause problems for consumers.

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 as existing federal statutes govern most uses of data and how it is gathered, collected and disseminated.

In conclusion, for all of the above reasons, we strongly oppose the bills and recommend studying this issue further. Thank you for your consideration of our comments and I would be happy to answer any further questions you may have.

Sincerely,

A handwritten signature in blue ink, appearing to read "Sarah M. Ohs".

Sarah M. Ohs

Director of Government Relations