SHANNON ZIMMERMAN

STATE REPRESENTATIVE • 30th ASSEMBLY DISTRICT

Assembly Bill 957
Assembly Committee on Consumer Protection
February 16, 2022

Thank you Chairwoman Dittrich and committee members for hearing testimony on Assembly Bill 957 today. I have dubbed this bill the Wisconsin Data Privacy Act because it will enshrine in Wisconsin statutes rights that will help consumers protect and control their personal data.

In short, the bill will allow any consumer in Wisconsin to ask a data collector what Personally Identifiable Information (PII) they have in their possession. The Department of Homeland Security defines PII as "any information that permits the identity of an individual to be directly or indirectly inferred". Beyond requesting a copy of the PII on file, consumers will be able to uncover how far and wide their information has been shared or sold. Finally, consumers will be able to request the deletion of their PII.

Americans have little faith that legitimate data collectors can collect and store data without that information falling into the wrong hands. A recent Pew Research poll indicated that 79% of respondents "are not too or not at all confident that companies will admit or take responsibility when they misuse or compromise data" and 81% "think the potential risks of data collection by companies outweigh the benefits". Even more astounding was the 81% of respondents who "believe they have very little or no control over the data companies collect about them".

Empowering consumers with the tools to control their personal data should be at the forefront of what we do in the Legislature. The adage, 'if you are not paying for the product, you are the product', has never been so true. Companies offer free products and services and in return, they are able to extract massive amounts of data from consumers. These companies then turn around and market that information to advertisers.

While the use of consumer personal data is ripe for abuse, technology still offers lifelines on many fronts. For example, the power of quantum computing can assist scientists and researchers in uncovering revolutionary findings. Curing cancer is legitimately on the horizon.

Thank you again for your time and attention to this proposal and I hope I can count on your support of this measure as we move forward.

P.O. Box 8953 • Madison, Wisconsin 53708-8953 • (608) 266-1526 • Toll Free: (888) 529-0030
Rep.Zimmerman@legis.wi.gov

WISCONSIN CABLE COMMUNICATIONS ASSOCIATION
22 East Mifflin Street, Suite 1010 - Madison, WI 53703 - 608/256-1683 - Fax 608/256-6222

Executive Director – Thomas E. Moore

Statement of Tom Moore

Executive Director, Wisconsin Cable Communications Association

RE: 2021 Assembly Bill 957

The Wisconsin Cable Communication Association is 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 Astrea.

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. Importantly, 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 like Charter, a search engine, an e-commerce site, a streaming service, a social network or a mobile 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. A few, like California, Colorado, Nevada, and Virginia have already passed legislation to do so. 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.

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. Privacy policies also should be separate from other terms and conditions of service. If all online companies provide this type of transparency, consumers will have a greater ability to weigh the potential benefits and harms of the collection and use of their personal data.

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. 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 hinders 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. A system filled with inconsistency or contradictions will not serve consumers, and will stifle technological innovation.

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.

We thank the Members of the Committee for the opportunity to submit written testimony, and look forward to continuing to work with you as you consider the right privacy regime to protect personal data for consumers in Wisconsin.

CR Consumer Reports®

February 15, 2022

The Honorable Barbara Dittrich, Chair
Committee on Consumer Protection
Wisconsin State Assembly
Room 17 West
State Capitol
PO Box 8952
Madison, WI 53708

Re: AB 957, Consumer Data Protection

Dear Chair Dittrich,

Consumer Reports[1] thanks you for your work on consumer privacy. AB 957 seeks to provide to Wisconsin consumers the right to know the information companies have collected about them, the right to delete that information, correction rights, and the right to stop the disclosure of certain information to third parties. However, in its current form it would do little to protect Wisconsin consumers' personal information, or to rein in major tech companies like Google and Facebook. The bill needs to be substantially improved before it is enacted; otherwise, it would risk locking in industry-friendly provisions that avoid actual reform.

Privacy laws should set strong limits on the data that companies can collect and share so that consumers can use online services or apps safely without having to take any action, such as opting in or opting out. We recommend including a strong data minimization requirement that limits data collection and sharing to what is reasonably necessary to provide the service requested by the consumer, as outlined in our model bill.[2] A strong default prohibition on data

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

[2] *Model State Privacy Act*, Consumer Reports (Feb. 23, 2021), https://advocacy.consumerreports.org/research/consumer-reports-model-state-data-privacy-act/.

sharing is preferable to an opt-out based regime which relies on users to hunt down and navigate divergent opt-out processes for potentially thousands of different companies.

Opt-out bills, like AB 957, are simply too burdensome for consumers to protect their privacy. Consumer Reports has found that consumers experienced significant difficulty exercising their rights under the CCPA's opt-out provision. In our study, hundreds of volunteers tested the opt-out provision of the CCPA, by submitting DNS requests to companies listed on the data broker registry. About 14% of the time, burdensome or broken DNS processes prevented consumers from exercising their rights under the CCPA.[3] Unfortunately, AB 957 lacks provisions, like a global opt-out and authorized agent rights, that will help make the CCPA more workable for consumers.

However, within the parameters of an opt-out based bill, we make the following recommendations to improve AB 957:

- *Require companies to honor browser privacy signals as opt outs.* In the absence of strong data minimization requirements, at the very least, consumers need tools to ensure that they can better exercise their rights, such as a global opt out. CCPA regulations *require* companies to honor browser privacy signals as a "Do Not Sell" signal; Proposition 24 added the global opt-out requirement to the statute. The new Colorado law requires it as well.[4] Privacy researchers, advocates, and publishers have already created a "Do Not Sell" specification designed to work with the CCPA, the Global Privacy Control (GPC).[5] This could help make the opt-out model more workable for consumers,[6] but unless companies are required to comply, it is unlikely that consumers will benefit. We recommend using the following language:

  > Consumers or a consumer's authorized agent may exercise the rights set forth in 134.985(2)(a)(1)-(5) of this act by submitting a request, at any time, to a business specifying which rights the individual wishes to exercise. Consumers may exercise their rights under 134.985(2)(a)(5) via user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt out.

---

[3] *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?*, Consumer Reports (Oct. 1, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-study-finds-significant-obstacles-to-exercising-california-privacy-rights/.

[4] Cal. Code Regs tit. 11 § 999.315(c); CPRA adds this existing regulatory requirement to the statute, going into effect on January 1, 2023, at Cal. Civ. Code § 1798.135(e) https://thecpra.org/#1798.135. For the Colorado law, see SB 21-190, 6-1-1306(1)(a)(IV)(B), https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_rer.pdf.

[5] Global Privacy Control, https://globalprivacycontrol.org.

[6] Press release, Announcing Global Privacy Control: Making it Easy for Consumers to Exercise Their Privacy Rights, Global Privacy Control (Oct. 7, 2020), https://globalprivacycontrol.org/press-release/20201007.html.

- *Broaden opt-out rights to include all data sharing and ensure targeted advertising is adequately covered.* AB 957's opt out should cover all data transfers to a third party for a commercial purpose (with narrowly tailored exceptions). In California, many companies have sought to avoid the CCPA's opt out by claiming that much online data sharing is not technically a "sale"[7] (appropriately, Prop. 24 expands the scope of California's opt-out to include all data sharing and clarifies that targeted ads are clearly covered by this opt out). We recommend the following definition:

> "Share" [or sell] means renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration, or otherwise for a commercial purpose.

While we appreciate that this measure has an opt out for targeted advertising, the current definition of targeted advertising is ambiguous, and could allow internet giants like Google, Facebook, and Amazon to serve targeted ads based on their own vast data stores on other websites. This loophole would undermine privacy interests and further entrench dominant players in the online advertising ecosystem. We recommend using the following definition:

> "Targeted advertising" means the targeting of advertisements to a consumer based on the consumer's activities with *one or more* businesses, distinctly-branded websites, applications or services, other than the business, distinctly branded website, application, or service with which the consumer intentionally interacts. It does not include advertising: (a) Based on activities within a controller's own *commonly-branded* websites or online applications; (b) based on the context of a consumer's current search query or visit to a website or online application; or (c) to a consumer in response to the consumer's request for information or feedback.

- *Non-discrimination.* Consumers should not be charged for exercising their privacy rights—otherwise, those rights are only extended to those who can afford to pay for them. Unfortunately, language in this bill could allow companies to charge consumers a different price if they opt out of the sale of their information. We urge you to adopt consensus language from the Washington Privacy Act that clarifies that consumers cannot be charged declining to sell their information, and limits the disclosure of information to third parties pursuant to loyalty programs:

---

[7] Maureen Mahoney, *Many Companies Are Not Taking the California Consumer Privacy Act Seriously, supra* note 3.

A controller may not discriminate against a consumer for exercising any of the rights contained in this chapter, including denying goods or services to the consumer, charging different prices or rates for goods or services, and providing a different level of quality of goods and services to the consumer. This subsection does not prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program. If a consumer exercises their rights pursuant to 134.985(2)(a)(5) of this act, a controller may not sell personal data to a third-party controller as part of such a program unless: (a) The sale is reasonably necessary to enable the third party to provide a benefit to which the consumer is entitled; (b) the sale of personal data to third parties is clearly disclosed in the terms of the program; and (c) the third party uses the personal data only for purposes of facilitating such a benefit to which the consumer is entitled and does not retain or otherwise use or disclose the personal data for any other purpose.

- *Remove the verification requirement for opting out.* AB 957 gives consumers the right to opt out of certain uses of the consumer's information. But it sets an unacceptably high bar for these requests by subjecting them to verification by the company. Thus, companies could require that consumers set up accounts in order to exercise their rights under the law—and hand over even more personal information. Consumers shouldn't have to verify their identity, for example by providing a driver's license, in order to opt-out of targeted advertising. Further, much of that data collected online (including for targeted advertising) is tied to a device and not an individual identity; in such cases, verification may be impossible, rendering opt-out rights illusory. In contrast, the CCPA pointedly does not tether opt out rights to identity verification.[8]

- *Strengthen enforcement*: We recommend removing the "right to cure" provision to ensure that companies are incentivized to follow the law. Already, the AG has limited ability to enforce the law effectively against tech giants with billions of dollars a year in revenue. Forcing them to waste resources building cases that could go nowhere would further weaken their efficacy. In addition, consumers should be able to hold companies accountable in some way for violating their rights—there should be some form of a private right of action.

We look forward to working with you to ensure that Wisconsin consumers have the strongest possible privacy protections.

[8] Cal. Civ. Code § 1798.130(a)(2).

Sincerely,

Maureen Mahoney
Senior Policy Analyst

cc: Members, Assembly Committee on Consumer Protection
The Honorable Shannon Zimmerman

February 16, 2022

The Honorable Barbara Dittrich
Wisconsin State Capitol
2 E Main Street
Madison, WI 53703

Dear Chair Dittrich:

BSA | The Software Alliance[1] supports strong privacy protections for consumers such as those in AB957. In our federal and state advocacy, BSA works to advance legislation that ensures Wisconsinites' rights – and the obligations imposed on businesses – function in a world where different types of companies play different roles in handling consumers' personal data. At the state level we have supported strong privacy laws in a range of states, including the new consumer privacy laws enacted in Colorado and Virginia last year.

BSA is the leading advocate for the global software industry. Our members are enterprise software companies that create the business-to-business technologies that other businesses use. For example, BSA members provide tools including cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal data — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security protections are fundamental parts of BSA members' operations, and their business models do not depend on monetizing users' data.

We appreciate the opportunity to share our feedback on AB957. Our recommendations below focus on our core priorities in the legislation – the sections concerning processors, treatment of employment-related information, and enforcement provisions.

I. Distinguishing Between Controllers and Processors Benefits Consumers.

We are writing to express our support for AB957's clear recognition of the unique role of data processors.

[1] *BSA's members include: Adobe, Alteryx, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.*

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

Leading global and state privacy laws reflect the fundamental distinction between processors, which handle personal data on behalf of another company, and controllers, which decide when and why to collect a consumer's personal data. Every state to enact a comprehensive consumer privacy law has incorporated this critical distinction. In Virginia and Colorado, new state privacy laws assign important – and distinct – obligations to both processors and controllers.[2] In California, the state's privacy law for several years has distinguished between these different roles, which it terms businesses and service providers.[3] This distinction is also built into privacy and data protection laws worldwide and is foundational to leading international privacy standards and voluntary frameworks that promote cross-border data transfers.[4] BSA and its members applaud you for incorporating this globally recognized distinction into AB957.

Distinguishing between controllers and processors better protects consumer privacy because it allows legislation to craft different obligations for different types of businesses based on their different roles in handling consumers' personal data. Privacy laws should create important obligations for both controllers and processors to protect consumers' personal data – and we appreciate AB957 recognition that those obligations must reflect these different roles. For example, we agree with AB957's approach of ensuring both processors and controllers implement reasonable security measures to protect the security and confidentiality of personal data they handle. We also appreciate AB957's recognition that consumer-facing obligations, including responding to consumer rights requests and seeking a consumer's consent to process personal data, are appropriately placed on controllers, since those obligations can create privacy and security risks if applied to processors handling personal data on behalf of those controllers. Distinguishing between these roles creates clarity for both consumers exercising their rights and for companies implementing their obligations.

II. Employment-Related Information Should Be Clearly Excluded from AB957's Scope.

We applaud AB957's focus on focus on consumers, who raise distinct privacy concerns than those raised by employees. We encourage you to retain both the exclusion for individuals acting in a commercial or employment context in the definition of "consumer" and the exclusion for employment-related data in Section 8(c)(15).

---

[2] *See, e.g.*, Colorado Privacy Act Sec. 6-1-1306; Virginia's Consumer Data Protection Act, Sec. 59.1-577.

[3] *See, e.g.*, Cal. Civil Code 1798.140(ag) (defining service provider and requiring service providers and businesses to enter into contracts that limit how service providers handle personal information).

[4] For example, privacy laws in Hong Kong, Malaysia, and Argentina distinguish between "data users" that control the collection or use of data and companies that only process data on behalf of others. In Mexico, the Philippines, and Switzerland, privacy laws adopt the "controller" and "processor" terminology. Likewise, the APEC Cross Border Privacy Rules, which the US Department of Commerce has strongly supported and promoted, apply only to controllers and are complemented by the APEC Privacy Recognition for Processors, which help companies that process data demonstrate adherence to privacy obligations and help controllers identify qualified and accountable processors. In addition, the International Standards Organization in 2019 published its first data protection standard, ISO 27701, which recognizes the distinct roles of controllers and processors in handling personal data.

III. The Attorney General Should Be Empowered to Enforce Comprehensive Consumer Privacy Legislation.

We support enforcement by the attorney general and applaud AB957 for providing the attorney general with the exclusive authority to enforce its provisions. We believe that a strong, centralized approach – with the state attorney general as the exclusive enforcement authority – is the best way to develop sound practices that protect privacy and encourage investment by companies in engineering that protects consumers in line with regulatory actions and guidance. State attorneys general have a track record of enforcing privacy-related laws in a manner that creates effective enforcement mechanisms while providing consistent expectations for consumers and clear obligations for companies. We also believe that if states enact new comprehensive privacy laws, the state attorney general should be provided with the tools and resources needed to carry out this mission effectively.

Thank you for your continued leadership in establishing strong consumer privacy protections, and for your consideration of our views. We welcome an opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,

Tom Foulkes
Senior Director, State Advocacy

20 F Street, NW, Suite 800
Washington, DC 20001

P 202-872-5500
W bsa.org

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

February 15, 2022

Representative Barbara Dittrich
Chair, Assembly Committee on Consumer Protection
Room 17 West
State Capitol
PO Box 8952
Madison, WI 53708
Via Email: Rep.Dittrich@legis.wisconsin.gov

RE: Assembly Bill 957

Dear Chair Dittrich:

On behalf of Microsoft, I am writing to support Assembly Bill 957 and applaud you for taking up the issue of data privacy. We would also like to thank Representative Shannon Zimmerman and Senator Dale Kooyenga for their leadership and commitment to advancing comprehensive privacy legislation. While the past several decades have brought dramatic changes in technology, U.S. law has fallen behind much of the world by failing to address growing challenges to privacy. There is widespread skepticism today that consumers can enjoy the benefits of technology while retaining control of their personal data and protecting themselves from harm. For those reasons, we need new privacy laws.

We support efforts to enact strong privacy protections in Wisconsin and believe that, in many respects, AB 957 would represent an important step forward. It would provide consumers with important rights to control their personal data, such as the rights of transparency, access, correction, deletion, and portability. It would provide consumers with the right to opt out of the processing of their personal data for targeted advertising, data sales, and profiling in furtherance of significant decisions such as the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health care services, or access to basic necessities. It would prohibit companies from processing consumers' sensitive data without consent. Finally, the bill would impose affirmative duties on companies to steward the personal data they collect responsibly.

We also have ideas for strengthening the bill's consumer protections, which we would be happy to share. For example, you could consider the following:

- Expand the definition of "sale" so that it includes the exchange of personal data for both monetary and "other valuable" consideration;
- Remove the concept of "pseudonymous data," which is unnecessary and potentially prone to abuse by those who might seek to avoid applying the consumer rights to modern data sets;

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Microsoft

- Expand the right to delete so that it would apply to personal data "concerning the consumer," thereby ensuring that the right would cover inferences about consumers derived from personal data;
- Explore mechanisms to make it easier for consumers to exercise their right to opt out of the processing of personal data for purposes of targeted advertising or the sale of personal data;
- Tighten and narrow the exemption for "publicly available information" so that such information would continue to be subject to key consumer rights that should pose few, if any, serious First Amendment concerns (such as the rights of transparency and access).

At Microsoft, we have long taken the privacy of our customers seriously, and we have a long track record of supporting responsible, thoughtful reform. Indeed, we have been calling for comprehensive privacy laws in the United States since 2005.

In short, we support your efforts to pass AB 957, and we look forward to working with you as the bill advances through the process. Thank you for allowing us to comment on this important issue.

Respectfully submitted,

Ryan P. Harkins
Senior Director, Public Policy
Microsoft Corporation