December 9, 2021

The Honorable Maria Cantwell
Chair, Senate Committee on Commerce, Science, & Transportation
254 Russell Senate Building
Washington DC, 20510

Re: Comments on the Consumer Online Privacy Rights Act (S.3195)

Dear Chair Cantwell:

The Software & Information Industry Association (SIIA) appreciates the opportunity to provide written comments on the Consumer Online Privacy Rights Act (S.3195). We believe there has never been a more pivotal time to establish an omnibus federal privacy law that would mitigate confusion and ease implementation across states.

SIIA is the principal trade association for the software and digital information industries worldwide. Our members include nearly 450 companies reflecting the broad and diverse landscape of digital content providers and users in specialized content industries, academic publishing, education technology, and financial information, along with creators of software and platforms used by millions worldwide, and companies specializing in data analytics and information services. As the only association representing a diverse array of technology companies, SIIA has long advocated for consumer privacy protections.

SIIA supports the enactment of a federal privacy bill and supports meaningful consumer safeguards and protections for individuals that also balance the practical needs of businesses. In drafting that legislation, the United States also has the benefit of being able to learn from both the mistakes and the successes of the GDPR.

GDPR has been successful in the sense that it has provided a uniform framework for regulating privacy. Where it has failed, however, is that its provisions impose burdens regardless of risk. It does not exclude any personal information, regardless of whether it is publicly available or if it is sensitive personal information, from its scope of application. Second, it mandates a blanket notice and consent, opt-in regime that does not, in most cases, actually protect privacy. There are strong indications that this approach has generated "consent fatigue" and complacency in a manner that does not further consumer protections. Third, it has imposed a strict liability regime (through contract) on firms regardless of their knowledge or control of another participant's acts in a particular information flow. These contracts are akin to intellectual property licenses, and breach of those contracts creates liability both under contract and a separate statutory regime. This construct has unnecessarily slowed down data flows and business transactions, and simultaneously created consent fatigue in consumer privacy decisions.

The current draft of S.3195 contains many of these same problems.

We recommend that the Senate advance a bill that remediates the shortcomings of the EU GDPR in order to provide more meaningful privacy protections to U.S. consumers and predictability to U.S. businesses, and foster innovation in a way the GDPR has not.

The remainder of this letter outlines specific recommendations on S.3195 designed to help achieve these objectives.

1. Exempt Publicly Available Information from the Definition of Covered Data

To a one, SIIA's members depend on the free flow of information. In order to perform valuable functions, they depend on a rich, robust public domain that contains information from two general categories of sources. The first involves information released by the government, whether through general publication or response to requests. The second involves information that is widely available in private hands for activities including research into case law and public records and news reporting, tracking down missing children, executing, and securing corporate transactions, compliance with know-your-customer laws, and the provision of so-called "alternative data" to inform trading decisions.

These valuable activities are not mere policy accidents: they are a direct result of a rich constitutional tradition that the European Union simply does not have. Strict scrutiny--the idea that a speech regulation must be narrowly tailored to address a compelling state interest--reflects a constitutional judgment that the United States regulates speech as a last resort, not a first one. Individuals therefore do not have a reasonable expectation of privacy in the First Amendment protected dissemination of publicly available information. In contrast, the GDPR presumes that the publication or use (e.g., "processing") of personal data is unlawful. The legal traditions approach privacy law from opposite poles.

S.3195 makes the same mistake. Like the GDPR, S.3195's duty of loyalty precludes any processing of covered information in violation of the Act. Section 101(a)(2). The Act provides consumers with several additional affirmative rights, including rights of access and transparency (Section 102), deletion (103), correction of inaccuracies (104), portability and opt-out (105), data minimization (106), and data security (107). The Act provides for enforcement through the FTC and private rights of action.

Section 2(8) of the bill defines "covered data" to include both information that identifies an individual or is reasonably linkable to an individual or a consumer device and includes "covered data that is created by the derivation of information, data, assumptions, or conclusions from facts, evidence, or other sources of information or data about an individual, household, or device used by an individual or household." *See* Section 2(11) (defining derived data).

"Covered data" does not include "public records," which the bill defines as information lawfully made available from government sources, provided that the entity processes and transfers such information in accordance with any restrictions or terms of use the government may place on it." Section 2(19). As an initial matter, therefore, the legislation covers only a part

of this broader domain: government information is fully outside its scope. Unlike every other piece of enacted legislation in this area, which exempts publicly available information from its scope entirely and defines it more broadly, S.3195 adopts a narrow definition. Section 2(18) of the bill defines "publicly available information" (PAI) as consisting of either information which a person has a "reasonable basis to believe" is publicly available, Section 2(18)(A)(i), or information that the person about whom the information relates directly had voluntarily disclosed to the general public. Section 2(18)(A)(ii).

The balance of the bill then subjects publicly available information to various exemptions. For example, the legislation carves out publicly available information from the rights of correction and deletion. Section 110(c)(3). It also exempts publicly available information from the rights of control. In addition, the bill does not require compliance with consumer requests if such requests impair the publication of newsworthy information, or if it would interfere with either the privacy of a third person or the rights of another to exercise free speech. Sections 110(c)(4), 110(c)(5). Prior consumer consent is not required at all to conduct "scientific or other research in the public interest" that meets standards of an institutional review board and other unnamed standards "promulgated by the Commission." Section 110(e)(1)(h). Although we appreciate the steps taken to mitigate the bill's effects on constitutionally protected speech, the legislation still has severe First Amendment problems that render it constitutionally defective.

First, the definition of publicly available information is too narrow. Information may "unreasonably" be believed to be in the public domain, yet under the statute it still qualifies as such. As importantly, that information is filled with information about people that they did not voluntarily release. And drawing inferences and publishing opinions about PAI, normally what our members think of as opinion, is regulated in a way that the First Amendment has never been held to allow. What's more, the legislation prohibits research based on large data sets unless that research has been approved by the FTC through what seems to be a standardless process. As a result, the definition of covered data has vagueness and overbreadth problems that would trigger strict scrutiny.

Second, despite its carve-outs, the bill also subjects publicly available information to other burdens, such as data minimization and security. And it does so not based on any particular use, but on the generalized belief that such information collected in large quantities presents a privacy violation. A generalized legislative concern over privacy is a legitimate government interest, but not a substantial or compelling one. *See U.S. West, Inc. v. FCC,* 182 F.3d 1224, 1235 (10th Cir. 1999) ("[P]rivacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it.").

To be clear, SIIA does not believe that all privacy regulation is unconstitutional, nor do we believe that a properly drafted bill would receive strict scrutiny. What we do believe, however, is that in order for S. 3195 to survive a facial First Amendment attack it must (as every enacted piece of general privacy legislation has done) carve publicly available information out from its sweep entirely. Not only would such a change insulate the statute

from a facial constitutional attack, it would free Congress's hands to protect truly private information and focus the legislation on information misuse.

2. <u>Extend Opt-Out to All Personal Information</u>

In today's digital ecosystem, businesses play multiple roles, as data controllers, processors, third parties, and contractors. Businesses and consumers would benefit from a streamlined process to allow consumers to opt out to certain uses of their sensitive personal information provided there is sufficient transparency built into the opt-out processes.

SIIA supports expanded individual consumer rights, as reflected in the draft legislation, including rights consumers should have to use, share, correct, retain and control their data, while ensuring it is being used fairly and limited to a specific purpose (Sections 101-107). SIIA also agrees with COPRA's general opt-out approach to consent for use of personal information, which would streamline business and consumer transactions and does not deviate too far from the state of existing, routine business transactions (Section 105). We propose revisions to strenuous opt-in requirements for data transfers focused on sensitive personal information (Section 105(c)), and instead, believe it would be beneficial to provide consumers with the option to make requests about their sensitive personal information, in lieu of an opt-in model.

There are numerous reasons why opt-in consent requirements can pose barriers. First, there are indications that opt-in consent has generated "consent fatigue" and complacency in a manner that does not further consumer protections. In particular, opt-in consent models could negatively impact historically marginalized communities of color and communities in poverty, who are more likely to face challenges with comprehending privacy policies and making notice-and-consent related decisions about their personal information, especially sensitive personal information. An example of an opt-in model that has resulted in these exact roadblocks is seen in the EU GDPR. The blanket opt-in has resulted in acute levels of consumer click-and-consent fatigue in today's fast-paced, tech-enabled environment and can have the effect of lessening, rather than increasing, the seriousness with which people take online privacy.

Second, consumers should have, at the very least, the option to determine whether they want their sensitive personal information shared. We need to future proof our privacy practices so that consumers are not shut out from basic activities, such as online banking, shopping, grocery delivery, and much more. We recommend an opt-out consent model, with a more tailored, risk-and-outcomes based framework that empowers consumers with options to learn about how their data is being used and to be able to act on this information.

For example, the narrow definition of sensitive personal information in Virginia's privacy law, the Virginia Consumer Data Protection Act (VCDPA) takes a beneficial approach, by upholding consumer rights and only including the most high-risk data in its definition of sensitive personal information. The definition does not include financial information and identification information, which provides more clarity for businesses and limits any overlap

regarding the way financial information is governed by other, existing state and federal laws. CPRA also defines sensitive personal information in a similar manner to S.2968 and establishes the consumers' right to limit use and disclosure of sensitive personal information. Notably, CPRA stops short of requiring opt-in consent on sensitive information; rather, it provides greater autonomy to consumers to request that their sensitive personal information is used "only for purposes necessary to perform the service or provide the goods requested or as prescribed by the CPRA or implementing regulations."[1]

Additionally, we recommend removing restrictions in Section 203, which would place additional requirements on the service provider before it can share consumer information with a third party. The provision requires service providers to gain opt-in, from the covered entity on behalf of the consumer, before transferring data to a third party. This additional request for consent would slow-down routine transactions for consumers, including across retail, banking, business operations and more -- a process that has been tested and faced with many subsequent negative repercussions in the UK, which is now making plans to reform its restrictive and cumbersome notice and consent procedures.[2]

Customers that currently benefit from tailored advertisements about their interests, choices, and experiences, may face consent fatigue from opt-in requirements in Section 203. Rather than creating a complacent culture of click and consent, we stand to gain by empowering consumers and giving them options to learn about the data being processed, should it be of interest to them. We recommend that Section 203 allow opt-out for service providers to share data with third parties, while granting permission to interested customers to request additional information on how the business, service provider and/or third party will limit the sale, sharing and use of their information.

In addition, it distinctly harms subscription businesses and businesses that provide ad-based services; these businesses may be required to adapt content to fit their customer's needs to ensure the safety and security of their customers (e.g., delivering age-appropriate content) and may have repeat customers that stand to benefit from tailored content.

Some of these businesses currently provide free or low-cost apps and services to their customers and generate the majority of their revenue from third-party advertising and marketing. Data analytics companies, market research firms, and related companies have business models that depend on efficient data flows between service providers and themselves, the third parties. All of these businesses would be crippled by an opt-in, which would likely lead to higher overhead and compliance costs, less revenue from advertising, and an existential threat to social media sites, mapping apps, food delivery subscriptions, and other common activities consumers engage in today.

---

[1] Bill Text. AB-694. Privacy and Consumer Protection: omnibus bill. CPRA.

[2] UK Department of Digital, Culture, Media and Sport, *Data, a New Direction* (Dec. 2020).

3. Strengthen Federal Preemption Language to Create Harmonized National Privacy Standards

As an association of both publishers and software providers, SIIA has seen how privacy regimes affect a wide variety of businesses--from the large platforms complying with different regimes around the globe, to the smaller business-to-business publishers that need only concern themselves with the law of a few states. All of our members believe that a single federal privacy law must harmonize the U.S. approach to privacy. In addition to learning from the GDPR's flaws, a federal privacy statute can emulate its successes. The GDPR created a single privacy standard for the European Union. Congress should do the same for the United States.

First, the processing of personal information is, quintessentially, interstate commerce, and businesses operating across state lines are tasked with compliance to a myriad of state consumer privacy laws - an onerous and expensive task, which should be streamlined and made more efficient through a uniform national standard. Second, a national standard would help resolve ongoing foreign commerce tensions with the EU over transatlantic data flows. From a global trade perspective, the Schrems II decision has pushed many companies towards data localization and created new barriers to entry. It would be valuable for the United States to build its own framework, which would further strengthen engagement with the EU on the need for an "adequacy" determination. United States adoption of a risk-based federal statute would offer meaningful privacy protection to US consumers, provide an alternative model to the EU's overregulation, and allow American innovation to continue to flourish. For this reason, a federal privacy law must provide for preemption of state privacy regimes, taking a centralized approach to privacy.[3]

SIIA recommends that the bill include strong federal preemption provisions to establish a harmonized set of privacy rules to govern activity across the United States. Doing so will enhance consumer protections and further the practical needs of industry by streamlining privacy compliance processes, creating predictability, and reducing redundancy and conflicts across other existing federal and state laws and regulations. This will create a strong privacy environment in the United States while avoiding the significant challenges to consumers and businesses alike from understanding and complying with myriad different privacy regimes across the country, which will increase costs to consumers and burden on business without increasing consumer protection and potentially stifling innovation.

To achieve this, Section 302 should be revised. As written, Section 302 suggests that federal privacy law would not override other existing federal laws and would *only* apply in the event there was a conflict with existing state laws. The ordinary meaning of those terms suggest that state laws will only face preemption if compliance with both the state and federal

[3] SIIA, Preemption and Privacy: Primer on Legal and Policy Considerations (2019).

statute is impossible. The result (except in rare cases) will be a continuation of the growing pandemonium of state regulation.

Absent a clear and uniform federal standard, S. 3195 will create limitless challenges and inconsistencies for businesses, consumers, service providers, and contractors, and it would likely exacerbate the current state of disconnected sectoral laws that apply unevenly to certain industries and data. If federal law does not supersede state law, it fundamentally stands in the way of clarifying how businesses and consumers must act, and what steps need to be taken to comply – which has a multiplier effect for businesses operating across more than one state. It also poses additional hurdles and could exacerbate existing business costs of compliance, implementation, and enforcement, which may then lead to a waterfall effect, where businesses would need to raise prices on consumers.

We have seen the challenges faced by businesses and consumers engaged in California, with many necessary amendments to the California Consumer Privacy Act (CCPA) that are now reflected in California Privacy Rights Act (CPRA). While consumer privacy laws in California, Virginia and Colorado have many similarities, the laws' unique definitions and terms (such as how they define data controllers and processors), unique thresholds for business requirements, and unique treatment and rules for processing sensitive personal information create variations that make it challenging for businesses and consumers alike. Both businesses and consumers will benefit from a uniform federal law that replaces the state-by-state patchwork that is beginning to develop.

We recommend revising Section 302 to reflect clear federal preemption of state law, modeling language in the Employee Income Retirement Security Act (ERISA), which regulates private sector employee benefit plans. A revised Section 302 should ensure that the federal law applies across states, industries, and sectors, with limited (but important) exceptions. These exceptions may include situations when states must retain authority over certain sectors such as wiretapping, the protection of Social Security numbers, identity theft, and student privacy. In most other instances, federal preemption has the potential to drive efficiency, reduce regulatory burdens and compliance costs in a patchwork of state policies, and increase the likelihood of smooth and expeditious implementation of the law across the country. We believe that a national standard is essential to promoting innovation in the information industry and protecting smaller businesses from undue compliance burdens.

4. <u>Avoid Unintended Consequences by Focusing the Bill on Technology-Neutral Framework</u>

SIIA has concerns that portions of S.3195 would create requirements for specific types of technology -- algorithmic decision-making and biometrics, in particular -- that could have serious unintended consequences. The definitions of these terms are so broad as to cover an incredibly wide swath of technologies and uses, including many that may be considered "low-risk" from the vantage of personal privacy. Yet, the bill does not incorporate a risk-based framework that would ameliorate some of the potentially deleterious effects. We also believe

that drafting would benefit from further education about the state of technology and how algorithms are used in generating different types of decisions and why there is importance in distinguishing among different technologies and data within the broader universe of biometrics.

In the meantime, SIIA strongly recommends that S.3195 avoid legislating on these processes or technologies in favor of establishing a strong, technology-neutral framework for privacy in the United States.

In the alternative, if these definitions and the relevant provisions are not removed, we recommend the following changes to lessen the risk that those provisions will lead to consequences that are harmful to consumer welfare and innovation.

a. <u>Refine the Definition of and Requirements for Algorithmic Decision-Making</u>

SIIA supports the need to provide essential protections to consumers against discriminatory and unethical uses of personal information, as set out in Section 108. SIIA also supports the need to provide guardrails around algorithmic decision-making. We note that a wide range of businesses today use algorithmic decision-making and that proposals to regulate artificial intelligence and algorithmic decision-making should be considered separately, so as not to conflate the presence and intent of data privacy laws. We believe that such proposals focused on algorithmic decision making should include a three-pronged approach:1) be future-proof, flexible and technology-neutral; 2) focus on a risk-based approach to decisions that leverage artificial intelligence and automated decision-making; and 3) use the risk-based approach to guide the use of impact assessments.

We respectfully recommend targeted revisions to Section 108 and to the definition of algorithmic decision-making in Section 2(1) that we believe will enable the legislation to better protect consumer privacy and ensure compliance by covered entities.

First, we recommend defining algorithmic decision-making to cover only those processes or techniques that make a decision. Our proposed revision is reflected by the strike-out language below:

> The term "algorithmic decision-making" means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques that makes a decision ~~or facilitates human decision-making~~ with respect to covered data.

This revision reflects the role of human input in providing guardrails and necessary checks and balances.

For illustration, we recommend the Committee look at the approach taken by the European Union in Article 22 of the GDPR on solely automated processes, which do not involve any human influence. Article 22 of the GDPR protects consumers from decisions "based solely

on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[4] As explained in guidance issued by the UK Information Commissioner's Office (ICO) on defining and determining the nature of automated decision-making processes in GDPR, the GDPR limits circumstances in which a business makes solely automated decisions, including those based on profiling.[5] The likely rationale for this guidance is to ensure that additional regulatory processes and scrutiny is focused on business decisions that are strictly based on automated processing, without a human to provide a check on the appropriateness of the decision.

Including in the definition the processes or techniques that "facilitate human decision-making" could render any computational technology (even a simple calculator) subject to the requirements for algorithmic decision-making set out in the act. This will create extraordinary burdens on the private sector without a noticeable return to consumer privacy. To the extent the Committee chooses to include in the definition of algorithmic decision-making those computational processes or techniques that facilitate human decision-making, we urge the Committee to refine the definition to avoid unintended consequences likely to result from the current definition.

Second, while we support the requirement of impact assessments set out in Section 108(b), the qualifier "perceived" in 108(b)(1)(B) is likely to increase uncertainty and render invalid or inaccurate decisions. We recommend striking the phrase "actual or perceived" from this paragraph. This approach is informed by the approach taken by the EU.

Third, we recommend that the Committee adopt a risk-based approach to impact assessments. We recommend that COPRA include direction to the FTC or another agency to establish guidelines for those situations involving algorithmic decision-making that are considered to be high-risk and warrant impact assessments, thereby exempting low-risk situations from the impact assessment process. This will help to focus resources on the areas of greatest need and greatest potential impact on individual consumers.

b. Refine Definition of "Biometric Information" and Provide Consumers with Expanded Choice on the use of Biometric Information

Technology companies recognize the important role they have when it comes to safeguarding consumer data, particularly sensitive biometric data. Biometrics have grown in use and availability, because of their high level of accuracy in identifying and authenticating individual human traits and their potential to further safeguard consumers' security and safety. Biometrics have become pivotal to authenticating customer identities in many daily operations: banking and retail activities, airport security, law enforcement and more. We believe that consumers should have individual rights to collect, retain, destroy and disclose

[4] GDPR, Article 22. Automated individual decision-making, including profiling.

[5] UK Information Commissioner's Office, What Does the UK GDPR Say About Automated Decision-Making and Profiling? (June 2018).

their biometric information and that businesses should be able to use biometric information to support and enhance a consumer's experience in business operations.

As an initial matter, we are concerned with the breadth of the definition of "biometric information" contained in Section 2(3), and the bill's classification of all biometric information as "sensitive covered data" under Section 2(20)(D). This definition will capture many types of data that are used to provide socially valuable services that do not raise concerns around privacy or civil liberties. In some cases, biometric information is used to ameliorate these types of concerns, for example, by correcting for unintended bias, providing increased data security, and authenticating users and digital information. We strongly recommend that staff undertake a thorough assessment of what is covered by this expansive definition and examine how broad definitions of biometric information under California and Illinois law have led to unintended and socially disfavored consequences.

In addition, we strongly recommend that the restrictions and obligations for sensitive data, as set forth in Section 105(c), incorporate a risk-based approach that recognizes that not all sensitive data -- including certain forms of biometric information -- present the same risks or concerns with respect to privacy.

SIIA also recommends that the federal privacy bill provide more flexibility to allow consumers and businesses to use biometric data for standard data processing and transfer practices, which, as noted, have become fairly routine in business-to-consumer (B2C) and business-to-business (B2B) operations. The research is clear that biometrics are the chosen form of identity verification by consumers[6]; therefore, businesses cannot take a step back, if they want to keep up with customer expectations for the use of biometric data.

To achieve this, SIIA recommends revising Section 110(d)(2) to remove the strict prohibitions on data processing and data transfer limitations on biometric data. The current draft includes strict limitations on data processing and data transfer. These limitations are likely to have unintended consequences that have a significant negative impact on consumer welfare.

An example of the clear and unintended consequences of overregulation of biometric data can be found by reviewing recent lawsuits of Illinois's Biometric Privacy Act (BIPA) law. In July 2017, for example, twenty-six class action lawsuits were filed by employees who claimed their employers violated BIPA's consent, notice, and disclosure policies because their time clocks required employee fingerprints.[7] There were no allegations that their biometric information was shared outside the confines of that relationship, that the employer used sub-standard security, or that their privacy was materially violated in any way. Similarly, in 2021,

---

[6] Thales blog (thalesgroup.com). *How biometrics help banks give consumers what they want*. (Feb 2017).

[7] IllinoisPolicy.org, *Illinois employers flooded with class-action lawsuits stemming from biometric privacy law* (October 2017).

numerous multinational companies using face and voice recognition technology to track employee performance have been flagged with similar violations.[8]

In addition, these strict limitations are likely to impede U.S. innovation and global competitiveness. Although adjacent to concerns around consumer privacy, innovation and competitiveness are important policy objectives that must be kept in mind in furthering legislation that will have a material impact on a data-driven world.

In place of strict limitations, we recommend directing the FTC to establish context-based restrictions on high-risk uses of biometric information and otherwise requiring opt-in consent from consumers, as appropriate, prior to the consumers' biometric data being transferred to a service provider, or before transfers take place between a service provider and a third party. Prudent, targeted restrictions on biometric information will promote security and consumer protection and not stifle efforts to innovate. Doing so will prepare the US, without unnecessary slowdowns or limitations, to effectively compete and remain secure in a highly advanced digital world, where data-driven technology is quickly becoming the norm for every consumer. It also allows the digital ecosystem to continue to leverage safe, secure, and high-quality biometric technology that benefits consumers and businesses alike.

SIIA would appreciate the opportunity to emphasize and share the state of existing common and best practices with regard to biometric information and commend staff for seeking to gather additional stakeholder input on this critical issue.

Conclusion

In order to undertake these efforts, we support the need for the FTC to create a new bureau to assist in exercising their authority under COPRA and other Federal laws addressing privacy, data security, and related issues. In addition, we endorse a federal privacy law that includes privacy practices that do not permit discriminatory or illegal practices.

We understand and appreciate the complexity of the issues this legislation raises and look forward to working with you as it moves forward.

Respectfully submitted,

Paul Lekas, SVP for Global Public Policy
Christopher Mohr, SVP for Intellectual Property and General Counsel
Divya Sridhar, Senior Director for Data Policy

Software & Information Industry Association (SIIA)

[8] SHRM, *TopGolf Settles Biometric Privacy Lawsuit* (July 2021).