1090 Vermont Avenue, NW, Sixth Floor
Washington, DC 20005-4905 www.siia.net

September 30, 2020

Via Email
Senator Reuven Carlyle
233 John A. Cherbourg Building
Olympia, Washington 98504

Re: 2021 Washington Privacy Act

Dear Senator Carlyle,

SIIA welcomes the opportunity to provide feedback on the first draft of the 2021 Washington Privacy Act. SIIA is the only trade association representing more than 700 companies across the global information industry. Our members reflect the broad and diverse landscape of the digital information age. This includes B2B and B2C services, from small and specialized firms to large multinational industry leaders – across finance, education, health, technology and specialized content and publishing. Many of our members do business in Washington, and will be subject to the 2021 Washington Privacy Act if it passes.

Our members create and provide a variety of publications and services incorporating public domain information, ranging from educational products to scientific, technical, and medical publishing to B2B publications (such as professional directories) to research tools. The value of these tools depends on their completeness and accuracy, and consists in large part of obtaining information that is publicly available from both government and non-governmental sources. These tools are used for many valuable activities, including academic research, fraud detection, news and financial reporting, locating missing witnesses, corporate transactions, law enforcement and antiterrorism activity, and other valuable uses. These tools are used by the federal government, and most likely Washington State itself.

SIIA supports the goals of the Washington Privacy Act, and believes both that privacy is critical to democratic decision-making and an appropriate and important focus of legislative activity. With that said, however, interests in privacy must be balanced against other core values, such as freedom of speech.

We are concerned that the Washington Privacy Act (WPA) does not properly calibrate that balance. It regulates "personal data," which it defines as any information that is linked or reasonably linked" to an individual.[1] The definition excludes publicly available information," which is defined as "information that is lawfully made available from public records."[2]

[1] S. 6281, § 3 (25) (a) (second substitute) [hereinafter WPA].
[2] *Id.* § 3(25)(b).

The WPA places certain obligations on publishers of personal information, including a right of correction,[3] a right to deletion,[4] and a right to opt out of the sale or processing of personal data.[5] In order to be subject to the legislation, a legal entity must either conduct business in Washington or target products or services to Washington residents *and* have information on at least 100,000 consumers.[6]

By its terms, the WPA affects a wide variety of information in which consumers have no reasonable expectation of privacy. SIIA's members publish bibliographies, databases of news and academic articles, and other kinds of compilations that look exclusively to publicly available information. While we applaud the exclusion for government records, the subjection of our members' publications to opt-out and deletion requests will result in holes in these and other important kinds of tools.

That kind of overbreadth raises more than policy problems—it renders the WPA constitutionally unsound. We therefore urge you to revise the WPA to fix this constitutional failure by expanding the exclusion for "publicly available information" to include information that is widely available in private hands. The balance of these comments explain why the WPA is unconstitutional, and proposes language that will cure that infirmity.

The First Amendment and Publicly Available Information

The constitutionally protected public domain consists of information from two sources. The first, which the WPA exempts, involves information that the government discloses. The second category, which is far larger, includes information widely available in private hands, such as that contained in and gleaned from newspaper and academic articles, professional directories, and specialized publications. While the government generally has a legitimate, perhaps even a compelling interest, in protecting privacy, a statute that protects privacy must still fit within the traditional First Amendment framework. As currently written, this legislation does not.

The WPA is Content-Discriminatory

The First Amendment protects the creation and dissemination of information. *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011) ("the creation and dissemination of information are speech within the meaning of the First Amendment.") (citing *Bartnicki v. Vopper*, 532 U.S. 514, 527 (2001) ("[i]f the acts of disclosing and publishing information do not constitute speech, it is hard to imagine what does fall within that category, as distinct from the category of express conduct.") (other citations omitted). Thus, the fact that a particular company must collect 25,000 pieces of information remains irrelevant to whether such information receives constitutional protection. *See Sorrell,* 131 S. Ct. at 2666 (rejecting lower courts arguing for lower scrutiny due to the fact that plaintiff aggregated information as a "commodity").[7] The fact that this information

[3] *Id.* § 6(1).
[4] *Id.* § 6(2).
[5] WPA § 6(5).
[6] WPA § 4(a)(b).
[7] While the Court in *Sorrell* did not rule on the state's request for a new exception to the historical categories of unprotected speech, it has repeatedly rejected such requests because of the risk that such a ruling would "matter to permit the Government to imprison any speaker so long as his speech is deemed valueless or unnecessary, or so long as an ad hoc calculus of costs and benefits tilts in a statute's favor." *United States v. Stevens*, 559 U.S. 460, 470–71 (2010).

may be sold for a profit similarly does not deprive it of constitutional protection. *Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105, 115 (1991).

The WPA, therefore, must satisfy First Amendment standards. Citizens engage in protected First Amendment activity when they publish news reports, disseminate information about financial transactions, share data from scientific experiments, or publish professional directories. The transmission of lawfully acquired information facilitates investigative journalism, assists law enforcement investigations, and forms the backbone of public social, political, and commercial discourse.

The standard applicable to the WPA is strict scrutiny.[8] The WPA's distinction between "information that is lawfully made available from federal, state, or local government records," which it does not regulate, and the broader public domain, which it does, represents classic content discrimination. The WPA would ban certain businesses from selling the "personal information" of people who exercise their statutory right to opt out. Such a law does not affect speech incidentally but instead directly "imposes a burden based on the content of speech and the identity of the speaker." *Sorrell*, 564 U.S. at 567. Through the deletion and opt-out provision the Act, "the government is prohibiting a speaker from conveying information that the speaker already possesses." *Id.* at 568 (internal quotation marks omitted). *See also IMDb.com Inc. v. Becerra*, 962 F.3d 1111, 1120 (9th Cir. 2020) (California statute requiring deletion of age from public web site subject to strict scrutiny). The distinction between government information and the broader public domain represents a classic example of content discrimination, and as such must be narrowly tailored to a compelling state interest.

As mentioned above, SIIA believes that privacy is and remains a legitimate, and occasionally important or compelling state interest. We note, however, that the government cannot defend a speech restriction "by merely asserting a broad interest in privacy." *U.S. West, Inc. v. FCC*, 182 F.3d 1224, 1235 (10th Cir. 1999). Here, the state simply asserts a general right of privacy in its citizens in public domain information—indeed, in a variety of information in which they have no legitimate privacy rights.

Even assuming that the state can plausibly assert a compelling state interest, the statute is fatally over and underinclusive. The same kind of speech that is prohibited by the act can be distributed by entities not subject to it. Thus, for example, a company that derives 49 percent of its revenue from the sale of personal information and contains the information of 99,000 consumers may refuse requests to delete a news article about a particular person from its academic journal database, while someone who derives 50 percent may not. And a company that distributes the same information obtained from government records is not affected at all no matter what its size, even though the "privacy injury" to the consumer is the same. The statute is also overinclusive as it targets information in professional directories, unrestricted social media feeds and blog posts, and other works in which the consumer has no reasonable expectation of privacy. As a result, the WPA impermissibly restricts speech without advancing a compelling government interest or engaging in the tailoring to meet that interest as required by the First Amendment. These flaws would doom the Act on its face.

---

[8] We note that a lower standard of scrutiny exists for information that does no more than propose a commercial transaction. *E.g., Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 562 (1980). The WPA standard affects speech that has nothing to do with such transactions, and as such the lower standard is inapplicable. Moreover, even if the lower standard of scrutiny applied, the WPA would not survive it.

The WPA Should Join the Legislative Consensus Around Widely Distributed Media

With that said, the WPA's First Amendment problems are eminently fixable, and a legislative consensus has emerged around a solution. Over the last year, an emerging consensus has formed that privacy regulation must address the First Amendment with respect to the entire public domain. For example, California is poised to amend the CCPA by passing the California Privacy Rights Act, which will exclude public records and widely distributed media from its scope in order to address First Amendment requirements.[9] The ballot initiative's backer has stated that the definition for publicly available information and its resulting exclusion was based on the need to meet First Amendment standards. In addition, the Uniform Law Commission's current draft of a model privacy law does the same.[10] Third, at the federal level, the SAFE DATA Act and the COVID-19 Consumer Data Protection Act of 2020 incorporate the same exclusion.

Thus, we believe that the most straightforward fix for the WPA's constitutional flaws is to expand the definition of "publicly available information" to include information from non-governmental sources. As a drafting matter, the solution is easy. Section 101(19)(b) should be revised as follows (with the new language in bold):

> "For purposes of this subsection, "publicly available information" means information that is lawfully made available from federal, state, or local government records **or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media."**

Like the GDPR and the CCPA, the WPA arises in a regulatory climate in which consumer information was collected in circumstances in which the consumer held a reasonable expectation of privacy, such as when online shopping at home. By adding the above language, the WPA would be limited to those areas in which such an expectation exists.

Thank you for the opportunity to provide you with our comments and suggested edits as you work to finalize the draft Act. We recognize that these comments raise significant concerns, and welcome a dialogue as this process moves forward.

Respectfully submitted,

/s/
Christopher A. Mohr
Vice President for Intellectual Property & General Counsel
Sara DePaul
Associate General Counsel & Senior Director for Technology Policy

---

[9] *See* "Inside the closed-door campaigns to rewrite California privacy law, again" available at: https://www.protocol.com/inside-california-privacy-law-redo.

[10] *See* Collection and Use of Personally Identifiable Data Act, September 17, 2020 Session, available at: https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=4efeec2c-dff8-742b-ca40-20a6bbbabaee&forceDialog=0.