ConnPIRG

Comments of Ed Mierzwinski, U.S. PIRG and ConnPIRG Federal Consumer Program Director
Before the Connecticut General Assembly General Law Committee

March 15, 2021

RE: SB 893 AN ACT CONCERNING CONSUMER PRIVACY

ConnPIRG is an advocate for the public interest, consumer protection, and a healthier, safer world in which we're freer to pursue our own individual well-being and the common good.

Concerns Regarding SB 893, An Act Concerning Consumer Privacy

I write on behalf of ConnPIRG and its members regarding SB 893, An Act Concerning Consumer Privacy. While we strongly support the need for passage of a consumer privacy law, SB 893 appears to be largely based on industry-supported, but generally consumer-opposed, proposals under continued consideration in Washington state and recently enacted in Virginia. The 2018 California Consumer Privacy Act, as amended by a 2020 ballot initiative, is a better starting point, although in no way perfect.

We concur with all of the concerns raised by the Attorney General in his testimony. Here are some additional, but by no means comprehensive, concerns:

One of the main problems with the Act is that it is based on the outdated "notice and opt-out" framework which underpins the current system of commercial surveillance and fails to provide consumers with meaningful control over their personal information. Consumers shouldn't be asked to opt-in or opt-out of harmful data sharing; it should simply be restricted.

SB 893 only gives consumers the right to opt-out of the "sale" (but not the collection) of certain of their personal information and then only for certain targeted advertising or profiling purposes, not for all secondary purposes. But, again, the debate shouldn't be about the form of consent.

Further, SB 893 does not give consumers a private right of action to defend themselves from privacy harms.

Instead, SB 893 grants exclusive enforcement authority to the Attorney General, but gives violators a so-called right to cure before the Attorney General can take action.

The bill would allow use of a “Pay for Privacy” regime in Connecticut, setting up a system of privacy “haves” and “have-nots.”

Further, the narrow definition of sale is a massive loophole. Among other exceptions, it does not include sharing with corporate affiliates. Then, other exceptions appear to effectively exempt Facebook and Google’s business models: Targeted advertising does not include “(a) advertisements based on activities within a controller's own Internet web sites or online applications or (b) advertisements based on the context of a consumer's current search query.”

SB 893 requires a consumer “to exercise the consumer rights authorized,” including the limited right to opt-out, but allows a data controller to reject “unauthenticated” requests.

SB 893 explicitly exempts not only activities covered by a variety of federal laws; it generally also exempts the entities. For example, the Gramm-Leach-Bliley Act is a federal law that imposes modest data protection and data breach rules on both banks and numerous non-bank “financial institutions” (these firms are those defined by an FTC interpretation of the Bank Holding Company Act). As the Attorney General pointed out at the hearing:

> “Notably, GLBA and HIPAA subject entities are not afforded blanket exemptions under other analogous state laws or proposals, (e.g. in California, Washington, and New York) and we would not recommend providing such a broad exemption here. Rather, the exemption should be specific to the information regulated by those laws, not the entities as a whole.”

Other federal data privacy laws that provide some or total exemption to entities and/or activities that would otherwise be covered by SB 893 include the Health Information Portability and Accountability Act (HIPAA), the Child Online Privacy Protection Act and the Fair Credit Reporting Act.

“Personal data” does not include de-identified data, which is subject to re-identification, or pseudonymous data. Personal data should capture any information that could be linked directly or indirectly to a person, household, or device. Separate storage of supposed pseudonymous data is an ineffective means of protecting data.

Sensitive data is supposedly “protected” but isn’t. All data can be “sensitive.” Even ostensibly innocuous data can be used to infer racial or ethnic origin, mental or physical health conditions, sexual orientation, or citizenship or immigration status. It does not

make sense to have a separate category of “sensitive data” that is treated separately in this bill.

The bill would allow a data controller to conduct its own data protection assessments that determine the benefits (and costs) of the collection and use of data to the consumer and other stakeholders. These are subject under the act only to review by the Attorney General, but not public disclosure.

Again, these are top-line concerns, but are not intended as a comprehensive overview of SB 893. ConnPIRG looks forward to working with the committee and legislature on further privacy laws, but cannot recommend advancing this proposal.

Sincerely,

Ed Mierzwinski, Senior Director U.S. PIRG Federal Consumer Program