Consumer Federation of America
1620 I Street, N.W., Suite 200 * Washington, DC 20006

Testimony of Susan Grant, Senior Fellow
Consumer Federation of America
To Rhode Island House Committee on State Government & Elections
In Support of H. 7917
March 30, 2022

On behalf of Consumer Federation of America (CFA), an association of nonprofit consumer organizations across the United States, I am submitting testimony in support of H. 7917, the Rhode Island Information Privacy Act. Founded in 1968 to advance consumers' interests through research, education, and advocacy, CFA strongly supports states' efforts to protect individuals' privacy. Unfortunately, some states have recently enacted laws that provide the illusion of privacy but actually do very little to protect their residents' personal information or reign in the troublesome data practices of companies such as Google and Facebook. H. 7917 takes a much better-informed approach and would provide real, effective privacy protection for Rhode Islanders.

A seminal survey conducted in 2019 by the Pew Research Center showed that, by large majorities, adults in the U.S. feel they have little or no control over the data companies collect about them, are concerned about how their data are used, and believe that the potential risks of such data collection outweigh any benefits they may derive from it. A strong majority also say that they have little or no understanding of what companies do with their data. Seventy-five percent said that there should be more government regulation over what companies can do with their personal information.[1]

It is not surprising that many people are in the dark about companies' privacy practices, because the system of commercial surveillance that has developed in the absence of comprehensive state or federal privacy laws is largely invisible to individuals. In many cases data is being collected about them by entities with which they have no direct relationship – for instance, by third-party "ad tech" companies that lurk on the websites they visit, and data brokers that obtain information about them

[1] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

from many different sources. Even entities with which people interact directly, such as Google and Facebook, are engaged in much more extensive tracking and profiling than users may realize, though that is changing as more scandalous revelations come out, seemingly weekly, about their data collection and use. A recent petition by the organization Accountable Tech asking the Federal Trade Commission (FTC) to initiate a rulemaking on "surveillance advertising" provides an excellent explanation of Google's and Facebook's business models and describes the commercial surveillance system more broadly.[2] To help policymakers understand this type of advertising and the concerns it raises, CFA has created factsheets and other materials, which are available at a central hub, https://consumerfed.org/surveillance-advertising-factsheets/.

It is not necessary to know individuals' names, physical addresses or phone numbers in order to collect their personal data and draw inferences about them and their households. As CFA's factsheet on tracking for surveillance advertising[3] explains, people can be tracked in a variety of ways without their knowledge as they go about their daily lives. Even when individuals are aware of the ubiquitous tracking that takes place in the commercial surveillance system, it is extremely difficult for them to avoid it and the profiling that it facilitates.

These profiles may not be accurate. For instance, a person could be shopping and doing other errands for an elderly relative, or researching a problem that a friend is experiencing, but the data that are collected through these activities may be linked to that person, not the relative or friend, through the device that is being used, an associated account, location data or some other type of information. Even if the assumptions made about the person are accurate, however, they may be unfair or undesirable. CFA's fact sheet on surveillance advertising and discrimination[4] provides examples of how profiling can result in opportunities for employment, housing and credit being presented to some individuals and not others, or some people being charged more than others for the same products or services. As CFA's general fact sheet about surveillance advertising[5] explains, these data practices can also be used to promote unhealthy products, encourage gambling, perpetrate fraud, and for other purposes that are very concerning. Furthermore, the enormous stores of personal data collected in the commercial surveillance system put individuals at risk for exposure, identity theft, and more malicious

[2] *See* https://accountabletech.org/media/accountable-tech-petitions-ftc-to-ban-surveillance-advertising-as-an-unfair-method-of-competition/.
[3] *See* https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-how-tracking-works/.
[4] *See* https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-discrimination/.
[5] *See* https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-what-is-it/.

tracking. In addition, their 4th Amendment rights may be eroded, as government agencies can purchase data from commercial sources that would otherwise require a warrant.

It is important to understand how this system works in order to develop public policies that effectively protect individuals from harm and ensure their fundamental rights to privacy are respected. Without that understanding, privacy legislation, though well-intentioned, is meaningless. For instance, the Consumer Data Protection Act (CDPA)[6] enacted in Virginia, which was written by Amazon[7] and is being promoted by Big Tech companies as a model for other states, allows broad collection, use sharing of individuals' personal information. While it gives individuals the ability to opt-out of "sale" of their data, "sale" is narrowly defined as the exchange of personal data for monetary consideration by the controller to a third party.[8] That is not how the commercial surveillance system generally works. It is not individuals' actual personal information that is being sold; it is their profiles, which are created by tracking them over time and space and which may be enriched with information from data brokers and other sources. CFA's diagram of how surveillance advertising works[9] illustrates this. Therefore, Virginians' right to opt-out of sale has little practical effect. Furthermore, the consideration involved may be not be monetary; it could be in the form of an exchange of services, for instance.

The right to opt-out of targeted advertising in the Virginia law also provides less privacy protection than one might assume. By excluding advertisements based on activities over time within a controller's own websites or online applications from the definition of targeted advertising,[10] Google and Facebook are not covered, despite the fact that their business models are based on collecting huge amounts of personal data from tracking their users' activities across their many websites and apps, profiling them, and delivering targeted ads to them on behalf of other companies.

The CDPA has many other serious shortcomings, including allowing individuals to be refused products or services, charged more, or provided with lower-quality products or services if they exercise their privacy rights.[11] Some contend that people are willing to trade their privacy for discounts or other

---

[6] CDPA, Code of Virginia, Title 59, Chapter 52, §59.1-571 through §59.1-581, available at https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+CHAP0036+pdf.

[7] *See* Jeffrey Dastin, Chris Kirkham, and Aditya Kalra, "Amazon wages secret war on Americans' privacy, documents show," Reuters (Nov. 19, 2019) available at https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/

[8] *Id.* §59.1-571.

[9] *See* https://consumerfed.org/consumer_info/factsheet-surveillance-advertising-diagram/.

[10] CDPA §59.1-571.

[11] CFA has pointed these out in a number of letters, press releases and opinion pieces. *See* https://consumerfed.org/press_release/virginia-legislature-ignoring-consumer-groups-steamrolls-bad-privacy-bill-

benefits. But as a study[12] conducted by Professor Joe Turow and colleagues at the University of Pennsylvania showed, people are not happy about making such trade-offs:

- 91 percent disagreed (77 percent of them strongly) that "If companies give me a discount, it is a fair exchange for them to collect information about me without my knowing."
- 71 percent disagreed (53 percent of them strongly) that "It's fair for an online or physical store to monitor what I'm doing online when I'm there, in exchange for letting me use the store's wireless internet, or Wi-Fi, without charge."
- 55 percent disagreed (38 percent of them strongly) that "It's okay if a store where I shop uses information it has about me to create a picture of me that improves the services they provide for me."

They concluded that conduct which has been misconstrued as trade-off behavior is actually due to the fact that "a large pool of Americans feel resigned to the inevitability of surveillance and the power of marketers to harvest their data."

With its narrow definitions, numerous exceptions and exemptions, and reliance on notice and opt-out rather than privacy by default, the CDPA fails to provide effective privacy protection and is *not* a good model for Rhode Island to emulate.

In contrast, H. 7917 requires individuals' informed consent to collect and process their data for the first time, for specific purposes, with common-sense exceptions for executing transactions for which they are providing their personal information, emergency situations involving immediate danger of death or physical injury, or where the data has been de-identified. It requires covered entities and data processors to process personal information and use automated decision systems only to the extent

---

toward-enactment/, https://consumerfed.org/testimonial/cfa-and-other-groups-weigh-in-on-va-privacy-bill/, https://www.virginiamercury.com/2021/02/16/we-need-real-privacy-protection-in-virginia/, https://roanoke.com/opinion/columnists/leech-grant-and-mierzwinski-privacy-law-isnt-strong-enough/article_ef16e92c-7d4c-11eb-a448-9f3858a2eb94.html, https://consumerfed.org/press_release/consumer-and-privacy-groups-urge-virginia-governor-to-veto-or-send-privacy-bill-back-to-legislature/, https://consumerfed.org/testimonial/cfa-urges-va-legislative-work-group-to-recommend-changes-to-strengthen-data-protection-law/.

[12] Joseph Turow, Michael Hennessy, and Nora A. Draper, *The Tradeoff Fallacy - How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation*, University of Pennsylvania Annenberg School of Communication (June 2015), available at https://repository.upenn.edu/cgi/viewcontent.cgi?article=1554&context=asc_papers.

necessary, to be honest about their data practices, to secure the data, and not to use the data in any way that would cause detriment to individuals or that they would not expect. It also requires that any third parties with whom the data is shared are contractually bound to the same duties of care, loyalty, and confidentiality, and that they be monitored to ensure compliance.

H. 7917 gives individuals the ability to see, correct, port and delete their data, and protects their ability to freely exercise their privacy rights by prohibiting threats, manipulation, or other unfair tactics. They would also have the right to know if their data will be subject to automated decision systems, whether it would be used for targeted advertising or monetization, and what types of third parties it is disclosed to, including government agencies. The bill prohibits denying products or services to people, charging them more, or giving them less if they exercise their privacy rights, but it does allow for bona fide loyalty club-type programs. It also protects individuals from data processing that would result in unlawful discrimination.

The definitions in the bill are appropriately broad to avoid creating loopholes for entities such as Google and Facebook. Importantly, its coverage includes biometric and location data, and it prohibits surreptitious surveillance though microphones, cameras, sensors or other devices. It also addresses workplace surveillance, providing for notice and reasonable limitations.

Unlike the Virginia law and bills in some other states, H. 7917 covers entities that are subject to federal laws to the extent that it provides stronger privacy protection than those laws do, and it while it supersedes state and local laws, regulations and ordinances, it makes exceptions for those that provide stronger privacy protection.

H. 7917 establishes a new privacy agency in Rhode Island that would develop regulations to help guide businesses, create model privacy notices, use its administrative powers to enforce the law, and educate the public. Crucially, individuals would also be able to enforce their rights under the law. The bill provides for reasonable penalties.

What it does *not* provide is a right to cure, something that Big Tech companies and the advertising industry will undoubtedly push for. The right to cure is not commonly found in other consumer protection laws and there is no reason why there should be such a right here. It essentially blocks any administrative or legal action until the covered entity has received a warning about a possible violation and has been given a certain period of time to “cure” it (a term that is never defined). This is a terrible idea for several reasons: it allows companies to avoid penalties, even for egregious violations, if

they claim to have stopped engaging in the violations and promise not to commit them again; it provides no public transparency in regard to companies' errant behavior; it results in no redress for individuals who have been harmed; it creates no legal precedents to guide enforcement agencies and businesses; and it provides no reimbursement for the costs of investigations, which can be substantial.

Rhode Island legislators will likely encounter resistance to H. 7917 from Big Tech companies and others engaged in the commercial surveillance system because it would require changes in their data practices. Without those changes, however, there can be no meaningful protection for individuals' personal information. There is no point in enacting legislation if it is simply a hollow gesture. H. 7917 is one of the best state privacy bills we have ever seen, and we will be happy to help promote its passage. Please contact me at sgrant@consumerfed.org with any questions you may have.