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

epic.org
ELECTRONIC PRIVACY INFORMATION CENTER

TO: Kimberly McCullough, Legislative Director
Kate Denison, Assistant Legislative Director
Oregon Attorney General's Office

FROM: Susan Grant, Senior Fellow, Consumer Federation of America
Caitriona Fitzgerald, Deputy Director, Electronic Privacy Information Center (EPIC)

RE: Comments on Oregon Comprehensive Privacy Law Draft

Date: June 3, 2022

Consumer Federation of America (CFA), an association of nonprofit consumer organizations across the United States, and the Electronic Privacy Information Center (EPIC), a nonprofit organization established in 1994 to protect privacy, freedom of expression, and democratic values in the information age, applaud the work of the Oregon Consumer Privacy Task Force in drafting a comprehensive privacy law. We strongly support states' efforts to protect the privacy of their residents' personal data and appreciate the thoughtful process through which this draft law was written. It is in many respects much better than most of the privacy laws that have been proposed or enacted in other states so far. There are, however, some changes that are necessary to avoid unnecessary loopholes and provide more effective privacy protections for Oregonians. Our suggestions are organized by following the sections in the draft.

Section 1. Definitions

(11) (a) Personal data

The definition of "personal information" in the California Consumer Privacy Act (CCPA) includes "Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes."[1] This is crucial because it is not always specific pieces of information about individuals that are being sold or made available on some other basis by businesses – it is the individuals' profiles, as CFA explains in a series of factsheets about surveillance

[1] Section 14 (v) (1) (K), available at https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#section14

advertising.[2] Without making clear that personal data includes such inferences, the Oregon law would fall short of fully encompassing modern commercial data practices.

(17) "Sale," "sell," "selling," "sold"

Oregon has the advantage of learning from the experiences of California, which passed the CCPA in 2018. Last year, voters approved a ballot measure, the California Privacy Rights Act (CPRA), which revised the CCPA in several respects, effective January 2023. One of those revisions was the addition of a definition for "share," "shared," or "sharing."[3] This addition was needed because some businesses were claiming that the ways in which they were benefitting from making Californians' personal information available to third parties did not come under the definition of "sell." The new definition for "share" specifically applies to situations in which the data is to be used for "cross-context behavioral advertising" (targeted advertising) "whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged." Without including a similar definition, the Oregon law would again fall short of fully encompassing modern commercial data practices.

(19) "Targeted advertising"

The essence of targeted advertising is delivering ads to individuals based on their activities over time and space. The data involved are not only used to predict individuals' preferences and interests, as the Oregon draft law states. They can also be used to determine the prices and terms to offer individuals, or groups of individuals, and the economic opportunities to present to them. Furthermore, these data are not only gleaned from individuals' activities over time across websites and in using apps; data from their communications, purchase histories, locations, and other activities over time in the physical world may also be used.

A better definition of targeted advertising can be found in S. 46, the Massachusetts Information Privacy Act,[4] which was introduced in that state's legislature last year:

> "Targeted advertisement" means an advertisement directed to an individual or group of individuals where the advertisement is selected by an automated decision system based on processed personal information obtained or inferred over time from the individual or the groups of individual's devices activities, communications, or associations across websites, applications, services, or covered entities.

It goes on to say that targeted advertising does not include advertisements directed to individuals solely based on their current interactions with a website, app, service, covered entity, or a direct response to individuals' requests for information or feedback – the reasonable exception for contextual advertising.

This definition is sufficiently broad to fully encompass modern commercial data practices and it avoids the loopholes that are created when the websites and apps are described as "nonaffiliated" or "distinctly branded." For instance, in using the term "a consumer's activities over time and across

[2] Available at https://consumerfed.org/surveillance-advertising-factsheets/
[3] Section 14 (ah) (1), available at https://www.caprivacy.org/annotated-cpra-text-with-ccpa-changes/#section14
[4] S. 46, Section 1 (a), available at https://malegislature.gov/Bills/192/SD1726

nonaffiliated websites or applications" in the definition of targeted advertising, the draft Oregon law is essentially saying that it is *not* targeted advertising when individuals are served ads based on their activities over time across *affiliated* websites or apps. But this is the business model of companies such as Google and Facebook. It cannot be the intention of the Oregon Consumer Privacy Task Force to essentially exempt those companies from being subject to the consumer's right to opt out of targeted advertising.

Section 2: Scope, Exemptions

As with the wording of definitions, exemptions in legislation can dramatically weaken consumers' rights and create an uneven playing field for businesses. Therefore, exemptions should be as few and narrow as possible. Federal laws typically create baselines for consumer protection, leaving states free to provide stronger protections unless specifically preempted.

(2) (d)

The exemptions in subsection (2) for data covered by certain federal laws are for the most part unnecessary and preclude Oregon from enacting stronger protections in those areas should they be deemed necessary now or in the future. Of particular concern is the exemption in (2) (d) for personal data covered by the federal Gramm-Leach-Bliley Act (GLBA).[5]

While GLBA prohibits financial institutions from disclosing nonpublic personal financial information to nonaffiliated third parties without providing consumers with a notice that they can opt-out, the definition of nonpublic personal financial information is very narrow, and consumers have no right to opt out of having their data shared with affiliates, or with other financial institutions for joint marketing of financial services. There is no right to access one's data, to know the specific third parties with whom one's data have been shared, to correct the data, or to delete data that are not necessary for the financial institution to retain. There is no right opt-out of targeted advertising or profiling, and as noted the opt-out right for disclosing one's data to others is quite limited. There are no prohibitions against processing individuals' sensitive data without their consent. There are no prohibitions against processing individuals' data in a way that results in unlawful discrimination. There are no prohibitions against using dark patterns to unfairly manipulate individuals. There is no protection against being denied services, charged a higher price, or receiving a lower quality of services if consumers assert their privacy rights. In short, GLBA is a privacy notice law, but it is not a privacy protection law.

The draft law attempts to deal with this by exempting personal data covered by GLBA "if this Act is inconsistent with the GLBA and only to the extent of the inconsistency." This wording is confusing. A more straightforward approach is found in the Massachusetts Information Privacy Act, which in Section 19 (b)[6] says:

> "This Chapter covers businesses that are subject to federal laws concerning the processing of individuals' personal information to the extent that (i) this chapter provides stronger privacy protections for individuals than those federal laws; and (ii) those federal laws do not explicitly preempt state laws."

[5] 15 U.S. Code, Section 6801 et seq., available at https://www.law.cornell.edu/uscode/text/15/6801
[6] *See* https://malegislature.gov/Bills/192/SD1726

It might be better to refer to *data* that are subject to federal laws rather than businesses, but the point is that any provision of the Oregon law that provides stronger privacy protection than a federal law should prevail. (In addition to GLBA, the federal Family Education Rights and Privacy Act is also of particular concern, as the explosion of third-party "ed tech" companies what provide programs for online learning has raised questions about whether their data practices are sufficiently regulated under that law.)

Section 3: Consumer Rights

(6) Right to opt-out.

In (6) (c), the right to opt-out of profiling is limited to "profiling in furtherance of decisions that produce legal or similarly significant effects concerning a consumer." What constitutes legal or similarly significant effects is not defined, as it is in some other state privacy legislation. For example, the recently enacted Colorado Privacy Act includes the following definition, which we recommend adding:

> "Decisions that produce legal or similarly significant effects concerning a consumer" are those that result in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health-care services, or access to essential goods or services."[7]

The larger question, however, is why shouldn't individuals have the right to opt-out of profiling, period? There can be reasonable exceptions, such as analyzing consumers' behavior and locations to detect possible fraudulent use of their payment accounts. But we believe that if individuals want to opt out of this automated processing for purposes that aren't necessary to protect them or fulfill their requests, they should have the right to do so.

Section 5: Controller Obligations

(3) (b) (C)

This says that the disclosure or transfer of personal data to an affiliate of the controller is not a "sale," in apparent contradiction to Section 1, subsections (17) and (20). Subsection (17) defines a sale as the "renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal data to a third party..." and subsection (20) includes "an affiliate of the processor or the controller" in the definition of "third party." We strongly support treating affiliates as third parties in this context.

Consider Google: its affiliates include Adsense, which provides advertising services; DoubleClick, a data broker; the app store Google Play; the entertainment hub YouTube; the Chrome browser; the Google Maps service; Nest, which offers internet-connected thermostats, security cameras, smoke detectors and other devices; the Waze navigation app; the health and fitness tracking app Fitbit; Socratic, a homework helper; Verily, which works on solutions that combine devices, software, medicine and professional care to help people do thing such as manage diabetes; Android, which dominates the smartphone market; Project Wing, a drone delivery service; and dozens and dozens of other companies.

[7] Colorado Privacy Act § 6-1-1303, available at https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_enr.pdf

Consumers don't necessarily know who these affiliates are or what they do. Furthermore, these affiliates don't necessarily all have the same privacy practices and policies. The bottom line is that consumers don't expect that their data will be sold to or shared with these companies and should at the very least be able to opt out.

(3) (c) (a)

By excluding ads based on activities within a controller's own Internet websites or apps from what is considered "targeted advertising," the draft law once again creates a giant loophole that excludes companies such as Google and Facebook, which track consumers' activities over their many websites and apps to profile them for profit, from the obligation to disclose their processing of data for such advertising and how consumers can opt-out.

The entire structure of Subsection (3) is confusing; (b) and (c) should probably be configured as subsets of (a), which would make it clearer that these practices are exempt from the disclosure requirements.

(4) (a) (A) (ii) (2)

It is ironic that the overall framework of the draft Oregon law allows businesses to collect, use and sell individuals' personal information by default, but it prohibits the platforms, technology or mechanisms that consumers can use to exercise their opt-out opt rights from being "on" by default. When consumers download browsers or other tools that are specifically designed to opt-out, such as the Electronic Frontier Foundation's Privacy Badger, they *are* making an affirmative decision to opt-out. The draft law should make this clear. Consumers should not be required to jump through multiple, unnecessary steps to exercise their opt-out rights.

Section 9: Enforcement

(1) Notice.

Though we are pleased that the draft Oregon law does not provide a "right to cure," the requirement to provide a notice of violation before any enforcement may be taken if the Attorney General deems a "cure" possible is still problematic. The concept of a "cure" is not typically found in consumer protection statutes, and nowhere in this draft or in any other state privacy legislation is what constitutes a "cure" defined.

State enforcement agencies do not bring formal legal action in response to every suspected violation of consumer protection laws. Individual consumer complaints to state agencies are usually resolved through mediation, and when there appears to be a pattern of unfair or deceptive practices, it is not uncommon for enforcement agencies to reach out to businesses to seek information and discuss resolving problems informally. When to do this is a judgement call that enforcement agencies are very experienced in making. There is no need to provide the possibility of a "cure" in this statute.

Another judgement call is how long to wait before the agency initiates formal enforcement action. A time period set by statute, such as 30 days, may not be appropriate in all cases, especially if the injury to consumers is great, the number of consumers impacted by the errant practices is rapidly increasing, or the consumers affected are particularly vulnerable.

Furthermore, the introduction of the "cure" in state privacy laws may open the door for businesses, if sued, to argue that enforcement agencies unfairly rejected their proposed cures. What is an acceptable cure? It may not be enough for a business to simply stop violating the law or to start complying with it – in some cases it may be appropriate for the business to disgorge data that it should not have collected, retrieve data that it should not have sold or shared, provide financial recompense to consumers, reimburse the Attorney General for the cost of the investigation, or incur penalties. It is unclear, however, what leverage the agency would have to achieve these results. We also note that there may be multiple violations involved.

In short, the provision for a "cure" is not necessary and would unduly complicate and delay enforcement action. The Oregon Consumer Privacy Law Task Force should stop perpetuating the concept of a "cure" and remove this section from the draft bill.

(3) Private right of action.

A private right of action is crucial for any consumer protection law to be effective -- it is the most important tool the Oregon Legislature can give Oregonians to protect their privacy.

Without broad enforcement, companies will assume there is a low risk of enforcement by the state. The Attorney General's Office will never have the resources to right every wrong. The effort that went into enacting a privacy law will be wasted, and large and powerful technology companies will continue to invade Oregonians' private lives, spy on their families, and gather their most intimate facts for profit. Private enforcement ensures that data collectors have strong financial incentives to meet their data protection obligations.

Private enforcement is not a new concept, nor is it one that large businesses are unaccustomed to dealing with. Many privacy laws have private rights of action, and these provisions have historically made it possible to hold companies accountable for their privacy violations. They include the Cable Communications Policy Act, the Video Privacy Protection Act, the Fair Credit Reporting Act, the Drivers Privacy Protection Act, and the Telephone Consumer Protection Act.

The damages set in privacy laws are not huge in an individual case. Still, they can provide a powerful incentive in large cases and are necessary to ensure that privacy rights will be taken seriously, and violations are not tolerated.

We strongly support including a private right of action in the statute.

Additional Issues

There are two other issues that we would like to raise. First, one of the most serious concerns about the processing of individuals' personal data is the potential for it to result in unlawful discrimination. While the draft Oregon law requires, in Section 8, that controllers conduct data protection risk assessments to determine if processing personal data for the purpose of profiling may present a risk of unfair treatment or unlawful disparate impact on consumers, there is no section that specifically prohibits discrimination, as is usually found in other state privacy legislation. This omission should be remedied.

One way to do this would be to mirror the provision in the Colorado Privacy Act,[8] which says in 6-1-1308 (6):

> "Duty to avoid unlawful discrimination. A CONTROLLER SHALL NOT PROCESS PERSONAL DATA IN VIOLATION OF STATE OR FEDERAL LAWS THAT PROHIBIT UNLAWFUL DISCRIMINATION AGAINST CONSUMERS."

A similar, but more expansive provision, can be found in Section 10 of the Massachusetts Information Privacy Act.[9]

Second, it is likely that some industry stakeholders will strongly argue that state laws should be harmonized and will push statutes such as the Virginia Consumer Data Protection Act (VCDPA)[10] to use as models.

While the desire for uniformity is understandable, it is also understandable for state legislators to want to provide the most effective privacy protections they can for their constituents. Simply following other states' laws for the sake of uniformity is short-sighted. States are the "laboratories of democracy" and should be free to find the best solutions to meet the needs of their residents. The VCDPA, which was written by Amazon,[11] is a very weak privacy law[12] and not a model for other states to follow. What proponents of the VCDPA are pushing for is not a law that best protects individuals' privacy, but one that does not oblige them or their member companies to change their current business practices.

Please do not hesitate to contact Susan Grant at sgrant@consumerfed.org and Caitriona Fitzgerald at fitzgerald@epic.org to discuss these recommendations.

[8] *See* https://leg.colorado.gov/sites/default/files/documents/2021A/bills/2021a_190_enr.pdf

[9] *See* https://malegislature.gov/Bills/192/SD1726

[10] Code of Virginia, Title 59.1, Chapter 53, available at https://law.lis.virginia.gov/vacode/title59.1/chapter53/

[11] Jeffrey Dastin, Chris Kirkman, Aditya Kalra, "Amazon wages secret war on Americans' privacy," Reuters (November 19, 2021), available at https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/

[12] Hayley Tsukayama," Virginians Deserve Better Than This Empty Privacy Law," Electronic Frontier Foundation (February 12, 2021), available at https://www.eff.org/deeplinks/2021/02/virginians-deserve-better-empty-privacy-law