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

January 24, 2020

Chairwoman Jan Schakowsky and Ranking Member Cathy McMorris Rodgers
House Committee on Energy and Commerce
Subcommittee on Consumer Protection and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chair Schakowsky and Ranking Member McMorris Rodgers:

On behalf of Consumer Federation of America (CFA), an association of consumer organizations across the United States representing the interests of millions of individuals, I would like to provide comments and suggestions on the draft privacy bill recently released by committee staff. First, I should note that there is much to like in this draft, though many of the best and most vital provisions are bracketed, indicating a lack of consensus on those issues. Some crucial sections, however, such as to provide for a private right of action and to bar federal preemption, are left entirely blank in the draft. And some of the provisions in the draft, such as the proposal that the Federal Trade Commission (FTC) approve self-regulatory guidelines, are simply unacceptable.

As concerns about privacy increase, spurred by research, investigative reports, and scandals such as the Facebook/Cambridge Analytica incident, your committee has an opportunity to propose common-sense baseline protections to ensure that individuals are treated fairly by entities that seek to profit from their personal information. The ability to use individuals' data for commercial purposes must be subject to respect for their fundamental privacy and human rights, which is the premise for the General Data Protection Regulation in Europe. Commercial interests do not outweigh those rights. This bill would need substantial changes to garner our support.

The following section-by-section comments are made to point out where we think that certain provisions of the draft bill are necessary in a federal privacy bill and where others are not warranted. Ultimately we hope that you will be able to put a bill forward that we can support.

SEC. 2. SENSE OF CONGRESS, PRIVACY BILL OF RIGHTS.

It is surprising that this section is marked [TBD] in the draft because the provisions of the bill should logically flow from its stated purpose. The introduction to the *Public Interest Privacy*

Legislation Principles[1] put forward by CFA and thirty-three other consumer, privacy and civil liberties groups provides a good template for this section:

> *Unregulated data collection and use in the United States has eroded public trust in companies to safeguard and use data responsibly. Surveys show that, while individuals often try to remove or mask their digital footprints, people think they lack control over their data, want government to do more to protect them, and distrust social media platforms. The current U.S. data privacy regime, premised largely upon voluntary industry self-regulation, is a failure. Irresponsible data practices lead to a broad range of harms, including discrimination in employment, health care, and advertising, data breaches, and loss of individuals' control over personal information. Existing enforcement mechanisms fail to hold data processors accountable and provide little-to-no relief for privacy violations. The public needs and deserves strong and comprehensive federal legislation to protect their privacy and afford meaningful redress. Privacy legislation is essential to ensure basis fairness, prevent discrimination, advance equal opportunity, protect free expression, and facilitate trust between the public and companies that collect their personal data.*

SEC. 3. TRANSPARENCY.

Transparency about covered entities' data practices is essential for individuals, regulators, watchdog organizations and others who have interests in knowing what they are doing with personal data and holding them accountable. It is, of course, not a substitute for adopting fair information privacy practices; rather it should reflect those practices.

We are therefore very concerned about Section 3 (1) (D) (ii), which requires the privacy policy to describe whether and how the covered entity "customizes products or services, or adjusts the prices of products or services for individuals" because we do not believe that those are appropriate practices. The idea of what is often referred to as "personalized pricing" pricing is particularly objectionable.

We support including the bracketed phrase "consumer score" in (D) (iv). Research[2] about this type of scoring and the lack of transparency in that regard has raised serious concerns about transparency and fairness which should be addressed by this legislation.

Categorizing some types of personal data as "sensitive" ignores the fact that even mundane information about an individual's personal activities, such as purchasing unscented soap, can be used to reveal very sensitive information, as the Target "pregnancy predictor" program so richly

---

[1] *See* https://consumerfed.org/wp-content/uploads/2018/11/public-interest-privacy-principles.pdf.

[2] *See* Pam Dixon and Bob Gellman, *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future* (April 2, 2014), World Privacy Forum, available at http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf.

demonstrated.[3] Therefore it is wrong to limit the requirement in (D) (i) that the covered entity describe in detail the purposes for which it processes the individual's data to that which is "sensitive." A privacy policy should clearly describe, in detail, all purposes for which any personal data may be processed.

The requirement in (H) to disclose processing for targeted advertising leaves out another potential use that should be highlighted, which is profiling. Profiling may be used for targeted advertising but it can have many other uses as well; for instance, to determine the availability of a product or service, the quality of the product or service, and the price or terms.

It would be better to have a separate subsection that requires disclosure about selling or sharing individuals' personal data, not just with regard to data brokers but that explains why and under what circumstances data may be sold or shared with any other party, for any purpose.

We applaud the proposal for the filings required under subsection (2) to be made public. This is essential for real transparency about covered entities' data practices.

Subsection (4) is highly problematic. Ultimately the principal executive officer must be accountable for meeting the requirements of this section. This is necessary to provide an effective incentive to ensure compliance.

This section illustrates why a private right of action is so important. We cannot expect government agencies that are empowered to enforce these provisions to be willing or able to take legal action in every instance in which violations are alleged. Individuals must be able to hold covered entities responsible for noncompliance. Their ability to do so benefits all of us because it results in needed changes to business practices. To deny individuals access to justice is fundamentally wrong and would greatly hamper the effectiveness of this and any other privacy legislation.

SEC. 4. PRIVACY PROGRAM.

As in other sections of the draft, it is crucial for the FTC or other responsible agency (we have long advocated for an independent data protection authority in the U.S. as exists in most other developed countries around the world) to be able to initiate rulemaking. We see no reason why the rulemaking authority should be limited as it is in this draft. The agency must have broad rulemaking authority to not only flesh out the requirement of the legislation but to respond to new issues that need to be addressed.

[3] Kashmir Hill, *How Target Figured Out A Teenage Girl Was Pregnant Before Her Father Did* (February 16, 2012), Forbes, available at https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#4a3778b26668.

Individuals' devices such as computers, cell phones, and internet-connected appliances are for all intents and purposes indistinguishable from the individuals themselves as sources of personal data, so it is logical to include "or consumer devices" in (2) (D) and other places where it is bracketed.

Compliance with (b) and (c) should not be based on annual revenue alone but should also be based on factors such as the number of individuals and devices from which the entity processes personal data annually.

SEC. 5. RIGHT TO ACCESS AND DELETE COVERED INFORMATION AND REQUEST CORECTIONS OF INACCURATE INFORMATION.

Again, "consumer score" is important to include in this section.

We appreciate the provisions in subsection (a) (4) which give individuals additional rights with regard to public information, but we are confused about whether the threshold based on the entities' annual revenue and the numbers of individuals or devices from which the entity processes personal data is intended to apply to both information brokers and other covered entities. We also question whether the threshold is too high.

SEC. 6. LIMITATONS ON PROCESSING OF COVERED INFORMATION.

This is one of the most important sections of the draft bill and indeed in any privacy legislation. The FTC or other responsible agency must be able to promulgate regulations in this regard. It is here that individuals' fundamental privacy and human rights should be front and center. The starting point must be that processing is limited has to be that which is necessary to fulfill the individual's request and for purely operational purposes such as fraud control.

At first blush, the language in (b) (1) appears to create a huge loophole, though it is tempered by the reference to (d) and the language in (b) (2), which explains what "within the context of the interaction" means. Nonetheless, the language in (b) (2) (A) does potentially create a huge loophole, as it is unclear what is meant by "expected in light of the nature of the individual's transaction or with the individual's existing relationship with the covered entity." We note that the draft bill calls for FTC "guidance" to clarify this. Guidance does not have the same legal weight as a law, however, and in any case (b) (2) (B) provides a list of activities that individuals would reasonably expect and that should not necessitate consent. In our view, (A) is unnecessary and is an invitation to exploitation.

We strongly object to the inclusion of (b) (2) (B) (iv), "internal data analytics for the purpose of [product development and improvement]." Individuals have no expectation or obligation to

help covered entities develop or improve their products or services; they can be offered an opportunity to opt into that use if they wish. As we will point out later, however, consent should never be sought for any actions that could lead to unfair treatment of an individuals.

We do not object to first-party marketing in this subsection as long as there is the ability to opt-out of it as provided in (c), which is currently bracketed. First party marketing is only acceptable if the individual has an existing relationship with the entity, another bracketed provision.

We agree that first-party tracking across third party websites, applications, etc. should only be allowed with the individual's express consent, another provision that is currently bracketed.

In (d), it is again very important to narrow what is deemed "consistent with the context of the interaction" and avoid any language that could create loopholes.

As noted before, carving out "sensitive information" as a discrete category does not protect individuals when other types of information are processed that can have a sensitive impact. We believe that affirmative consent should be required for any processing that is not necessary to fulfill the individual's request and for purely operational purposes such as fraud control. In addition, we agree that consent is necessary when there are any material changes to the processing of covered information.

Again, rulemaking authority is absolutely necessary to set out how affirmative consent should work in practice. We find the fact that (e) (2) is in brackets mindboggling. Does someone seriously object to individuals being able to withdraw consent as easily as they gave it?

In (f), prohibited information processing practices are described. It may be a drafting error, but (1) (B) is about obtaining covered information under false pretenses, while (1) (B) (i) has nothing to do with that; it is about processing that the covered entity should not do except to the extent to which it is necessary to provide or add to the functionality of a product or service the individual has requested or is "consistent with the reasonable consumer expectations within the context of the interaction between the covered entity and the individual." This list which includes biometric information, precise geolocation, the contents of communications, health information, and covered information to attribute a "[consumer device or devices] to a specific individual using probabilistic methods" is good. In the exceptions (again there is a numbering/lettering problem, as this is (3) but there is no (2), though (2) is referred to here) it is not clear from the wording whether complying with "investigations" would require a court order or other "properly executed compulsory process." It should.

It is mystifying that the provision prohibiting a covered entity from seeking to obtain the individual's consent to engage in any of these prohibited processing practices is bracketed. Individuals should not be asked to agree to practices that public policy deems unacceptable.

We note that other prohibited processing practices are found in Section 11, which appears to be entirely bracketed. These have to do with discriminatory use of data, which is a crucial element of any privacy legislation. We will discuss this further in that section.

SEC. 7. DATA RETENTION.

Limits on data retention are a basic component of fair information practice principles. They protect individuals from unauthorized disclosures and inappropriate data use. We would prefer that this say something to this effect:

> *A covered entity shall not keep, retain, or otherwise store covered information for longer than is necessary to provide the product or service that the consumer has requested or for which the consumer has given specific consent.*

Exceptions such as those in Section 7 (a) (2) are reasonable but should be qualified by saying that the data shall only be retained for as long as necessary for those purposes.

SEC. 8. LIMITATION ON DISCLOSING COVERED INFORMATION TO PROCESSORS AND THIRD PARTIES.

It is unclear what is meant by the reference in (a) (B) to subparagraph (A), since there does not appear to be a subparagraph (A). Nonetheless, we believe that individuals' personal data should only be disclosed to processors or third parties for the purposes we have previously described. It is essential that those entities be required to comply with the same privacy and security protections.

It is also essential for the covered entity to perform reasonable due diligence to ensure that those parties are in compliance. We strongly object to the provision in (a) (5) that the covered entity should promptly take steps to ensure compliance if it has actual knowledge that a processor or third party has violated the law. This is a high bar that can be used as an excuse to escape responsibility for taking action. The standard should be that the covered entity has a reasonable belief that the party is in violation.

The exceptions in (b) raise the issue of whether data can truly be "pseudonymized." We believe that it cannot.

SEC. 9. DATA SECURITY.

Data security is another essential component of fair information privacy practices. While it may be reasonable for regulations in this regard to take into consideration certain factors regarding

the covered information involved, issues such as "the cost of implementing such safeguards" raise serious concerns. It is up to the covered entities to decide what their business models will be and what processing of individuals' persona data is necessary for those business models, subject to the limitations that are public policy places on them. If they cannot afford to secure that data, they should not be processing it.

We support the creation of a registry of information brokers as proposed in (c). Individuals are unaware of these entities and the vast amount of personal data they trade in. We also agree that individuals should have the right to delete the data held by such brokers. Here, and in the definition of covered data generally, we believe that "publicly available" should not include information collected by a business about an individual without that person's' knowledge. Use of such information can have very sensitive impacts on individuals and they should be able to block its sale for commercial purposes that are not necessary for uses such as fraud control.

[SEC. 11. PROHIBITION ON DISCRIMINATORY USE OF DATA.]

We do not understand why there is apparently a lack of consensus that individuals should be protected from discriminatory uses of data about them. This is one of the most serious concerns about the commercial use of personal data, especially in the advent of technology that makes automated inferences about individuals, inferences which can have profound impacts on their lives.

We would like to see a more expansive basis on which to rest the vital protections in this section, such as:

> *A person's or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability.*

[SEC. 12. ADDITIONAL PROHIBITIONS.]

Again, this crucial section is inexplicably bracketed. The current "take it or leave it" proposition that individuals face with regard to processing their data is unacceptable. This section, however, is not as comprehensive as it should be, since the discriminatory practices described in Section 11 narrowly cover only economic opportunities and housing. There many other ways that individuals can be treated unfairly, with no protection or control. We would like to see provisions here along these lines:

(a*) A covered entity shall not discriminate against an individual because the individual exercised any of the rights under this title, including, but not limited to, by:*

(1) Denying goods or services to the individual.

(2) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(3) Providing a different level or quality of goods or services to the individual.

(4) Suggesting that the individual will receive a different price or rate for goods or services or a different level or quality of goods or services.

(b) This title shall not be construed to prohibit a covered entity from offering discounted or free goods or services to an individual if the offering is in connection with the individual's voluntary participation in a program that rewards participants for repeated patronage, if personal information is used only to track their participation for loyalty rewards, and the covered entity does not share the individual's data with third parties pursuant to that program except for purposes of servicing the program.

(c) Except as provided in (b) a covered entity shall not ask the individual to waive the rights guaranteed by this Act.

SEC. 13. FTC APPROVED COMPLIANCE GUIDELINES

This section is absolutely unwarranted and unacceptable, and it is disturbing to see that it is not in brackets, as opposed to many of the most privacy-protective provisions of the draft bill. In the late 90's, the FTC encouraged self-regulation to address concerns about privacy, but by the year 2000 the agency concluded that self-regulation was not adequate and recommended federal privacy legislation.[4] In the absence of a comprehensive federal privacy law, the FTC has continued to encourage adherence to fair information practice principles and used the limited authority at its disposal to combat unfair or deceptive privacy and security practices.

There is no reason, for the FTC to approve voluntary guidelines for processing individuals' personal information. The text of any federal privacy law should be clear about the rights and responsibilities of the parties and covered entities should simply comply with the law.

We have no objection to self-regulatory programs that help covered entities understand that they should do under the law and that might even encourage participants to go further than the law requires. But there is no need to create a safe harbor for self-regulatory programs, and we strongly object to the notion that if self-regulatory guidelines are insufficient adherents to them have a "right to cure," essentially a free pass to escape liability for having violated the law. This proposal would add layers of complexity to the law and weakens enforcement.

[4] Federal Trade Commission, *Privacy Online; Fair Information Practices in the Electronic Marketplace* (May 2000), available at https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf.

SEC. 14. BUREAU OF PRIVACY.

As we noted before, we believe that the United States should have a data protection agency that has the necessary expertise, resources and powers to address the broad set of issues and challenges related to data privacy and security.[5] The FTC has many other responsibilities, including combatting fraud and anticompetitive marketplace conduct, fighting misleading advertising, and overseeing a host of important rules. Creating a dedicated agency that can focus solely on data protection, as exists in most other developed countries in the world, makes more sense than retrofitting the FTC for this purpose.

SEC. 15 ENFORCEMENT.

This section is weak in many respects. The inclusion of civil penalties is welcome but the amount is relatively low, especially when one considers that penalties under the GDPR can go up to four percent of the covered entity's worldwide revenue.

We welcome the fact that the draft bill provides for enforcement action by state officials, but we are concerned about limitations such as that in (b) (6) which appears to prevent a state attorney general from hiring a private person to bring a civil action on its behalf. It is not uncommon for attorneys general to retain outside counsel when they need that expertise and assistance and there is no reason to prohibit that.

The biggest problem is the fact that a private right of action is bracketed and blank. No federal or state agency will be willing or able to bring legal action in every instance where it may be merited. Individuals deserve to be able to enforce their rights. Private rights of action can not only remedy individual problems but in many cases they can change business practices for the benefit of all. Access to justice is a fundamental American value. Depriving individuals of that ability is wrong and weakens enforcement.

The bracketed provisions for rulemaking considerations are unnecessary and unhelpful. The FTC and other federal agencies are already subject to standards for rulemaking and adding further potential hurdles does not further the public interest.

[SEC. 16. RELATION TO STATE AND OTHER FEDERAL LAWS.][PREEMPTION.]

This bracketed section is also crucial to the effectiveness of this and any other federal privacy legislation. We want a federal bill that creates a strong baseline for privacy protections with the specific ability for states to go further. States have been in the forefront on data protection, from data breach notice requirements to data security, data broker registration to fair practices concerning certain types of data such as biometrics. They are often referred to as the "laboratories of democracy" for their ability to respond quickly to concerns of their residents

[5] *See Failures of the Current System: The United States Needs a Data Protection Agency* and other fact sheets about privacy on Public Citizen's website at https://www.citizen.org/wp-content/uploads/migration/fact_sheets_-_privacy_digital_rights.pdf.

and to innovate when new issues need to be addressed. No federal privacy law should preempt the states.

A federal privacy bill should also not exempt entities that are covered by other federal laws if the privacy protections extended by those laws are not as strong. A good case in point is Gramm Leach Bliley, which does not provide the same level of privacy protection for customers of financial institutions that sections of this and some other privacy bills. For instance, the burden rests on those customers to opt-out of their personal information being shared with third parties.

SEC. 17. DEFINITIONS.

We would like to flag issues with some of the definitions, but we note that a revised bill may necessitate other changes and additions in the definitions. We would be happy to work with committee staff in this regard.

Some of the definitions should be broadened. For instance, based on suggested language from other sources, biometric information could be defined as:

> *An individual's physiological, biological or behavioral characteristics or an electronic representation of such, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.*

We welcome common carriers being included in covered entities but we that all commercial entities should be covered.

Covered information should be expanded to include information that "identifies or could reasonably be linked, directly or indirectly, with a particular individual, household or device."

It is reasonable to include deidentified information in the definitions, but as noted before we do not support including pseudonymized information because we do not believe that it is feasible.

We are confused by what is meant by (11) (D) concerning health information. If this has to do with direct-to-consumer genetic testing services, it should "that was provided by an individual or a member of the individual's family" because while individuals may buy the kits on the basis of a seeing an advertisement, they may also receive them as gifts. In either case, they providing personal information when they send in the samples from which the test results are derived.

The definition of reasonable consumer expectation in (20) is missing the important qualifying phrase and subsequent language that appears in Section 6 (b) (2) (B). We have already expressed concern about (2) (A). Without narrowing it this definition is far too vague and broad.

Selling data should be broadened to include "for other valuable consideration, or otherwise for a commercial purpose."

Again, we believe that sensitive information is a misnomer, as even uses of mundane information can be "sensitive."

We are very pleased that third party includes affiliates. There is no practical reason why they should be exempt from following the law in regard to their relationship with individuals, which is no different than the relationship that third parties have with individuals.

Other important sections such children's privacy and relationship to existing law covering communications are left blank. Clearly this bill is unfinished, but it remains to be seen what its ultimate shape will be. In the meantime, other bills have emerged, some of them very good.[6]

Because of the important role that this committee plays in matters concerning commercial practices, it should lead the way with a bill that is centered on respect for individuals' human and privacy rights and that protects them from unfair and inappropriate treatment driven by commercial interests. We are grateful for your request for input and look forward to working with you to develop good legislation that we can support.

Respectfully,

Susan Grant
Director of Consumer Protection and Privacy
Consumer Federation of America

[6] See *Grading on a Curve: Privacy Legislation in the 116th Congress* (December 2019), Electronic Privacy Information Center, available at https://epic.org/GradingOnACurve/EPIC-GradingOnACurve-Dec2019.pdf.