The Honorable Frank Pallone, Jr., Chairman, House Committee on Energy and Commerce
The Honorable Greg Walden, Ranking Member, House Committee on Energy and Commerce
The Honorable Jan Schakowsky, Chairwoman, Subcommittee on Consumer Protection and Commerce
The Honorable Cathy McMorris Rodgers, Ranking Member, Subcommittee on Consumer Protection and Commerce
2125 Rayburn House Office Building
Washington, D.C. 20515

January 24, 2020

Via email

Dear Chair Pallone, Chair Schakowsky, Ranking Member Walden, and Ranking Member McMorris Rodgers:

Thank you for the opportunity to comment on the staff draft of a bipartisan digital privacy bill. This comment offers some top-line remarks on the draft bill. Some of us will also offer separate comments in the coming days.

We understand that this draft is meant to provide a starting point for discussion. For consumers, this bill does not qualify as a starting point. Its protections are well-meaning, but not meaningful, and its unfinished nature makes substantive discussion of its provisions speculative at best. We urge that this draft be replaced with a robust framework to protect consumers.

Among our key concerns with the draft:

- Consumers are demanding that Congress step in to end the current environment of rampant data-collection and corporate surveillance. This bill does not do enough to change the way companies behave. The provisions in the bill, particularly section six, double down on the notice and choice framework that has ruled since the beginning of the internet, and that perpetuates a myth that consumers have meaningful choice over how much they are surveilled. This section, the core of the bill's framework, aims to improve on the current situation by limiting data collection particularly by second and third parties, but the exceptions built into the rules severely limit their effectiveness. Even though this section is built on good intentions, it does not go nearly far enough to outweigh the rest of the bill's flaws.
  A bill that would truly protect consumers would be built on the principles of data minimization and fair information practices and would have sufficient enforcement mechanisms to hold powerful companies to account for their misdeeds. This bill does not come close.
- The bill does not do enough to protect civil rights and vulnerable populations. Artificial intelligence is used to determine more and more of our life choices, and without transparent and accountable civil rights protections, we risk cementing even further inequities and the most insidious biases in our society. We must not let algorithms limit anyone's life chances or foster discrimination.

- The failure to decide on anti-preemption and private right of action in the language limits our ability to evaluate the provisions in the rest of the bill. The real-world effects of the bill will vary based on the form of enforcement, so without knowing whether there will be a private right of action for consumers or what form that private right will take there is no way to know whether the provisions in the bill will be effective and how they will affect the consumer experience.
- Also left unfinished is the vital issue of whether the states should have the freedom to make digital privacy laws tailored to their own populations. We believe that there should be a baseline level of protection for all individuals in the United States, and that individual states should continue to take the lead on crafting protections that are the right fit for their populations.

For concrete ideas on a more consumer-friendly approach, please see the attached framework for model legislation from the Digital Rights for All Coalition.

We thank you for taking the time to read and consider these comments and the others that signatories will soon submit. Though our comments are critical, we do want to recognize the hard work of the staff that put this effort together. We share the goal of enacting strong federal baseline legislation, and we look forward to working with you in the future on a bill that will better protect consumers in the digital environment.

Sincerely,

Campaign for a Commercial-Free Childhood

Center for Digital Democracy

Consumer Action

Consumer Federation of America

Public Citizen

U.S. PIRG

Privacy and Digital Rights For All Model Legislation Outline

May 1, 2019

1. Findings (modeled on the Privacy Act of 1974)

a. The Congress finds that—

i. privacy is an important fundamental individual right protected by the Constitutions of the United States;

ii. the right of privacy is widely recognized in international legal instruments that the United States has endorsed, ratified, or promoted;

iii. the right to privacy protects the individual against intrusions into seclusion; protects individual autonomy; safeguards fair processing of data that pertains to the individual; advances the just processing of data; and contributes to respect for his or her civil rights and fundamental freedoms;

iv. privacy protections not only protect and benefit the individual, but they also advance other societal interests, including the protection of marginalized and vulnerable groups of individuals, the safeguarding of other foundational values of our democracy, such as freedom of information, freedom of speech, justice, and human ingenuity and dignity, as well as the integrity of democratic institutions, including fair and open elections;

v. the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information;

vi. the increasing digitalization of information and its application in classifying and predictive analytics has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

vii. the opportunities for an individual to secure employment, insurance, credit, and housing, and his or her right to due process, and other legal protections are endangered by the unrestricted collection, disclosure, processing and misuse of personal information;

viii. information systems lacking privacy protection amplify bias;

ix. in order to protect the privacy of individuals, it is necessary and proper for the Congress to regulate the collection, maintenance, use, processing, storage, and dissemination of information;
x. a violation of any provision in this Act constitutes a concrete injury as it would expose an individual to a risk of subsequent harm that Congress sought to prevent.
xi. Advances in digital technology and communications have enabled businesses to collect, maintain, use, and disseminate massive amounts of personal information about individuals.
xii. Businesses require individuals to provide their personal information in order to receive offers for and purchase goods and services, or to pursue employment opportunities.
xiii. Individuals do not lose their legitimate privacy interest in their personal information by providing such information, and they expect businesses that collect, maintain, use, and disseminate personal information to do so consistent with their legitimate privacy interests.
xiv. Individuals have a legitimate privacy expectation that businesses will not collect, use, or disseminate personal information about them unless they have provided explicit consent.
xv. When individuals who seek to engage in commerce or seek employment provide personal information, they retain legitimate privacy expectations that the businesses with whom they have entrusted their personal information will:
    1. only collect personal information that is necessary for the purpose for which it is collected and only use that information for the purpose for which it is collected.
    2. not disclose that personal information to unauthorized third parties.
    3. implement reasonable and adequate safeguards to prevent the unauthorized use, destruction, or disclosure of such information;
    4. not take action inconsistent with individuals' inalienable right to control their personal information, including the right to make corrections to their personal information and to require such businesses to delete personal information upon request.
    5. keep them informed of policies, practices, actions, and events affecting the security or other aspects of their personal information.
xvi. Throughout our nations' history, federal and state laws, including common law, have recognized and sought to protect individuals' legitimate privacy interests through mechanisms tailored to the specific privacy risks faced by individuals.
xvii. The rapid pace of advances in digital technology and communications over the past decades has made existing privacy protections inadequate to vindicate individuals' legitimate privacy interests.
xviii. Absent new enforcement mechanisms, the increasing collection, maintenance, use, and dissemination of individuals' personal information on a large scale will erode individuals' ability to maintain control over their personal information and to manage the risks associated with the disclosure of such information.
xix. Individuals who provide personal information to businesses expect those businesses to adhere to applicable privacy laws.
xx. Violations of privacy laws by businesses betray the trust of individuals who have entrusted businesses with their personal information, infringe on individuals' legitimate privacy interests, and violate the terms under which the individuals agreed to provide their personal information.

xxi. The disclosure of personal information to third parties is an especially egregious privacy violation because it results in personal information being made available to parties other than the business to which the individual entrusted the information.

xxii. Such disclosure can occur when a business knowingly transmits personal information to third parties (whether or not for compensation) or when its fails to implement reasonable and adequate safeguards to prevent the unauthorized disclosure of personal information to third parties (including unauthorized business employees and outside "hackers").

xxiii. The unauthorized disclosure of personal information deprives the individual of control over who has access to personal information, resulting in substantial emotional distress and anxiety, and creates a significant risk of reputational or financial injury to the individual that is often difficult to ameliorate.

xxiv. In addition, a business's failure to provide individuals with information required by law deprives the individual of making an informed decision about whether to entrust or continue entrusting the business with personal information.

xxv. Similarly, a business's failure to respect an individual's right to have personal information corrected or deleted deprives the individual of the ability to minimize the risk of financial or reputational harm from the business's or a third party's use of that information.

xxvi. Individuals who are the victims of privacy violations should be compensated for the time and resources needed to mitigate the risks associated with violations of privacy laws and to attempt to restore their privacy to the extent possible.

xxvii. More stringent privacy protections are needed for minors, who generally lack the cognitive maturity to understand fully the privacy implications of authorizing businesses to collect, maintain, use, or disclose personal information and lack the legal capacity to consent to such activities.

xxviii. The collection of personal information from large numbers of individuals has enabled businesses to conduct sophisticated analyses for purposes of creating algorithms designed to tailor the goods, services, or employment opportunities that will be offered to individuals, as well the prices, terms, or conditions of such offers.

xxix. Such analyses and algorithms are often considered confidential and propriety by the businesses that use them, notwithstanding the significant affect they have on the prices, terms, or conditions that may be made available to consumers.

xxx. Absent transparency and accountability, there is a substantial risk that such algorithms will incorporate biases that discriminate against certain groups of consumers or job seekers, especially those belonging to marginalized and vulnerable groups, on the basis for prohibited characteristics or other impermissible factors.

xxxi. Sophisticated data analyses of personal information are often viewed as inherently objective and unbiased, raising the risk that analyses incorporating incorrect or incomplete data, or faulty, imprecise, or biased assumptions, will produce a discriminatory effect that will be hard to detect before harming a large number of individual consumers or job applicants.

xxxii. Although various federal and state laws prohibit discrimination on the basis of race, religion, sex, and other characteristics in housing, credit, employment, and other areas, additional public and private enforcement mechanisms are needed to ensure that algorithmic decisionmaking does not produce the discriminatory effects that anti-discrimination law are intended to prohibit and that individuals

who are denied opportunities because of discriminatory algorithms obtain redress for that harm.

2. **Definitions**
    a. **"Automated Decision,"** means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making.
    b. **"Covered entities"** means any person that collects, processes, or otherwise obtains personal information with the exception of a person processing personal data in the course of exclusively personal or household activity.
    c. **"Explicit Consent"** means a freely given, specific, informed and unambiguous indication of wishes by an individual, either by a statement or by a clear affirmative action, signifying clear agreement to personal data relating to them being collected or processed. The statement to obtain explicit consent must specify the nature of the data being collected, the purpose of the collection, the details of any automated decision and its effects, or the details of the data that are going to be processed and the risks of said processing. Explicit consent must be revocable. (from the British ICO interpretation of GDPR)
    d. **"Legitimate Purpose"** means processing is necessary for the purposes of the legitimate interests pursued by the covered entity or by a third party, except where such interests are overridden by the rights of the individual which require protection of personal data, in particular where the individual is a child.
    e. **"Manipulation"** means the applications of information technology that impose hidden influences on individuals, by targeting and exploiting their vulnerabilities.
    f. **"Person"** means any natural or artificial person, partnership, corporation, trust, estate, cooperative, association, foundation, non-profit organization, or other entity.
    g. **"Personal Data"** means any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household, including but not limited to:
        i. an identifier such as a real name, alias, signature, date of birth, gender identity, sexual orientation, marital status, physical characteristic or description, postal address, telephone number, unique personal identifier, military identification number, online identifier, Internet Protocol address, email address, account name, mother's maiden name, social security number, driver's license number, passport number, or other similar identifiers;
        ii. information such as employment, employment history, bank account number, credit card number, debit card number, insurance policy number, or any other financial information;
        iii. medical information, mental health information, or health insurance information;
        iv. commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
        v. professional or employment-related information;
        vi. characteristics of protected classes under Federal law, including race, color, national origin, religion, sex, age, or disability;
        vii. biometric information;
        viii. internet or other electronic network activity information, including browsing history, search history, content, and information regarding an individual's interaction with an internet website, mobile application, or advertisement;
        ix. historical or real-time geolocation data;
        x. audio, electronic, visual, thermal, olfactory, or similar information.

xi. education records;
xii. political information;
xiii. password-protected digital photographs and digital videos not otherwise available to the public;
xiv. information on criminal convictions or arrests;
xv. information that allows an individual or device to be singled out for interaction, even without identification (includes IP addresses and other similar identifiers)
xvi. inferences drawn from any of the information identified in this subparagraph to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

h. **"Processing"** means any operation or set of operations on personal data, either manually or by automated means, including but not limited to collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, sorting, classifying, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

i. **"Profiling"** means the automated processing of data (personal and not) to derive, infer, predict or evaluate information about an individual or group, in particular to analyze or predict an individual's identity, their attributes, interests or behavior.

j. **"Sensitive Data Uses"** means the processing of information or data revealing race, color, ethnicity, religion or creed, national origin or ancestry, sex, gender, gender identity, sexuality, sexual orientation, political beliefs, trade union membership, familial status, lawful source of income, financial status (income level, assets), veteran status, criminal convictions or arrests, citizenship, past, present, or future physical or mental health or condition, psychological states, disability, geospatial data, or any other factor used as a proxy for identifying any of these characteristics; or the use of biometric or genetic data.

k. **"Third party,"** means any person that is not—

(A) the covered entity that is disclosing the personal data;

(B) solely performing an outsourced function of the covered entity disclosing the personal information if—

(i) the person is contractually or legally prohibited from using, retaining, disclosing, or selling the personal information after the conclusion of the outsourced function; and

(ii) the person is complying with the regulations promulgated under this Act; or

(C) a person with respect to which the individual gave specific opt-in approval for the covered entity to disclose the personal data of the individual to the person. (adapted from Markey bill)

3. Individual Rights

a. Right to obtain specific and transparent information abaout whether personal data is collected, the purpose of processing, who is using the data and what for, how long it will be retained, whether it will be transferred to a third party, and whether disclosure is voluntary - at time when data is requested or obtained
b. Right to access or obtain data about individual in possession of controller (whether directly obtained from controller or by third party)
c. Right to challenge denial of access

d. Right to have consent tied to specific purpose
e. Right to have personal data
    i. Erased
    ii. Corrected
    iii. Completed
    iv. Amended
f. Right to withdraw consent
g. Right to object
h. Right to restrict processing in certain circumstances (such as when processing is unlawful or the accuracy is contested. Personal data can be stored but not further processed until the issue is resolved.)
i. Right to avoid automated decision making and profiling, and request human intervention in automated decision-making and profiling.
j. Right to seek redress (see section 11)

4. Data controller obligations

a. The right to data privacy is a fundamental human right. Covered entities may only process data if there is a legal basis to do so, including
    i. On the basis of freely given, specific, informed, unambiguous, and revocable consent, or explicit consent if for sensitive data use purposes
    ii. If necessary for the performance of a contract
b. Data controllers must ensure the fair and just processing of personal data
    i. Require covered entities to regularly audit their data processing practices for bias, discriminatory impacts and privacy risks.
    ii. Require covered entities to release comprehensive annual privacy reports for researchers and regulators.
    iii. Covered entities must completely disclose how they collect and use personal data, including their algorithmic processing practices.
    iv. Covered entities must enable researchers to independently test and audit platforms for discrimination.
c. Transparency about business practices
    i. Openness about developments, practices, and policies
    ii. Establish data retention schedules
    iii. Existence of data systems
    iv. Purpose of use of data
    v. Identity and location of data controller
    vi. Unique children's privacy policies employed on all sites and platforms used by children
    vii. On package/retail website in clear language on any IoT device what info is collected, how it's used, if third parties have access
d. Data Collection limitations
    i. Limits on collection - collection limited to minimum necessary for legitimate purpose
    ii. No data collected until meaningful, informed, explicit, and revocable consent is obtained except for routine uses.
    iii. Requires 'unbundling' of each required consent
    iv. Lawful collection (does not fall under prohibited practices)
e. Data Minimization and Deletion

i. Data controllers should maintain only the minimum amount of information "relevant and necessary" to accomplish its purposes.
ii. Data minimization applies to the use, collection, and disclosure of data by controllers and their agents.
iii. Data deletion
    1. e.g.,"Destroy personally identifiable information as soon as practicable, but not later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information" Video Privacy Protection Act, 18 U.S. Code § 2710(e).
iv. Promote privacy innovation, such as privacy by design and data minimization techniques.

f. Purpose specification
    i. Specific purpose stated
    ii. Purpose specified at time of collection
    iii. Subsequent use only if consistent with purpose
    iv. New purpose specified for new use, new consent required
g. Accountability
    i. Data controller is specified
    ii. Compliance is required
    iii. Accountability mechanisms are established, including documentation, reporting, commensurate resources and accountable staff, privacy enhancing design and innovation, and data breach notifications.
    iv. Obligation for on-going confidentiality, integrity, availability and resilience of processing systems and services
h. Confidentiality/Security
    i. Protection against loss
    ii. Protection against unauthorized access
    iii. Protection against unauthorized destruction
    iv. Protection against unauthorized use
    v. Protection against unauthorized modification
    vi. Protection against unauthorized disclosure
i. Data accuracy
    i. Data is relevant for purpose
    ii. Data is necessary for purpose
    iii. Data is accurate
    iv. Date is complete
    v. Data is up-to-date

5. Prohibited practices/Limits on Data Uses and Disclosures

a. Prohibited Practices
    i. Prohibit re-identifying personal information.
    ii. Prohibit take-it-or-leave-it or pay-for-privacy terms.
    iii. Prohibit disclosure of information to third parties without explicit consent.
    iv. Prohibit manipulative advertising and marketing practices.
    v. Prohibit sensitive data uses unless:
        1. the individual has given explicit consent for such processing; or
        2. processing is carried out in the course of legitimate activities by a not-for-profit entity with a political, religious, or trade union purpose, on the condition that the processing relates solely to the members or former

members of the entity and the personal data is not disclosed to parties outside of the entity.

vi. Prohibit uses that affect legal rights or have a similarly significant effect (i.e. has the potential to significantly influence the circumstances of the individual), for example:
    1. Prohibit profiling of children under 18 or decisions about children and minors based on profiling, including the use of behavioral advertising;
    2. Prohibit targeted marketing to minors;
    3. Prohibit the use of personal data to discriminate in employment, housing, credit, education, or insurance—either directly or by disparate impact.
    4. Prohibit any uses that affect civil rights;
    5. Prohibit the use of personal data to engage in deceptive voter suppression;
    6. Prohibit the use of personal data to discriminate in public accommodations and extend such protections to businesses that offer goods or services online;

b. Limits on data uses
    i. Presumption against disclosure or new use of personal data inconsistent with purpose specification
    ii. Any collection of personal data must be relevant for purpose
    iii. Narrow exceptions for "internal" uses
    iv. Limits on profiling (used in scoring/predicting and ad targeting)
        1. Limits on profiling that affects legal rights or similarly significantly affects the individual or groups of individuals
            a. Includes: offline legal rights apply online
            b. Significance in terms of
                i. Invasiveness and counter-intuitiveness
                ii. Expectations
                iii. Exploitation
                iv. Relevance
                v. Accuracy and statistical reliability
        2. Targeted advertising may not limit life chances and opportunities (e.g., housing, employment, finance, education, health and healthcare, insurance, welfare benefits, "modern eligibility" for identify verification and fraud risk assessments)
    v. Limits on use of socio-economic indicators, race, and other protected classes as defined by anti-discrimination law
    vi. Limits on data uses required for high risk data processing
c. Use/disclosure Limitations
    i. Narrow exception for explicit consent of individual
    ii. Consent does not permit prohibited uses
    iii. New use inconsistent with original purpose requires new consent
    iv. Narrow exception for legal authority
    v. Enhanced limits on the collection, use and disclosure of data of children and teens
    vi. Requirement to disclose what third parties have access to children's data even if it is claimed it's for "internal purposes"

6. Data security and Privacy Innovation

a. Require Privacy enhancing techniques
b. Privacy by design as an affirmative obligation
c. Mandatory encryption
d. Privacy settings by default to be the most privacy-protective options
e. Promote privacy innovation

7. Algorithmic Governance

a. Transparency: Data inputs and algorithms be made available to the public, which gives individuals the right to know the basis of an automated decision that concerns them. Additionally, companies must regularly audit their algorithms for bias and discriminatory impacts and publicly release the results.
b. Accountability: Entities that improperly use data or algorithms for profiling or discrimination should be held accountable, particularly for misuse of data concerning marginalized and vulnerable populations. Individuals should have legal remedies for unfair and unjust decisions and outcomes. They should be able to easily access and correct inaccurate information about them. Accountability requires:
    i. Ex ante impact assessments of high risk data processing
    ii. Ex post outcome audits
    iii. Ongoing adjustments of data practices
c. Oversight: Independent mechanisms should be put in place to assure compliance with these requirements (the integrity of the data and the processing of the data at all stages). These mechanisms should help ensure the accuracy and the fairness of the decision-making and their fair and just outcomes. Additionally, companies must enable researchers to independently test and audit algorithms for bias and discrimination.
d. Applies to processing of aggregate and de-identified personal information
e. Protection of trade secrets and confidential business information may not override accountability requirements.

See Wyden Bill:
https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf

8. Establishment of an independent U.S. Data Protection Agency

a. Endow with commensurate resources for oversight and enforcement; develop multidisciplinary capabilities.
b. Assess current threats to data protection in the U.S.
c. Enforce privacy statutes and rules as authorized by Congress, with a broad range of tools including civil penalties, injunctive relief, and equitable remedies.
d. Rulemaking authority - promulgate rules to protect the privacy and security of individuals' personal information.
e. Ensure that privacy practices and processing are fair, just, and comply with Fair Information Practices. Regulate consumer scoring and other business practices that diminish people's life chances.
f. Oversee companies' ex ante impact assessments and ex post outcomes audits of high-risk algorithms and data practices to advance fair and just data practices.
g. Examine the social, ethical, economic, and civil rights impacts of high-risk data processing and propose remedies.

h. Ensure fair contract terms in the market, including the prohibition of "pay-for-privacy provisions" and "take-it-or leave it" terms of service.
i. Promote privacy enhancing techniques, such as privacy by design and data minimization techniques.
j. New high-risk techniques/applications (ad techniques and other profiling, e.g. scoring) must be reviewed and approved by DPA. In the DPA's discretion, a public rulemaking process may be conducted before approval.
    i. Special consideration to:
        1. sensitive data uses;
        2. children, minors;
        3. neurological, psychological data, insights/inferences, applications.
k. Issue opinions and other forms of guidance on complying with privacy and security obligations and on innovating to address emerging privacy challenges.
l. Take complaints and information from the public on data protection matters and respond to complaints.
m. Make annual reports to the public and Congress on the state of privacy in the United States and issue other reports as appropriate.
n. Participate in federal agencies' rulemaking concerning the Privacy Act and other federal privacy laws and in trade negotiations.
o. Resources dedicated to the unique concerns of marginalized and vulnerable populations, separate offices with multidisciplinary expertise, including
    i. Dedicated, separate office for children and teens and
    ii. Dedicated office for marginalized populations
p. Convene public workshops and conferences, conduct polls and engage in other types of research, meet with stakeholders, and conduct other activities as needed to obtain information and public input on data protection issues.
q. Represent the U.S. at international data protection meetings.
r. Provide the annual assessment for the Privacy Shield and other privacy related treaty obligations.
s. Create and disseminate public education materials.

See H.R. 685 (102nd Congress): https://www.congress.gov/bill/102nd-congress/house-bill/685

9. Federal enforcement and oversight

a. **A clear basis for enforcement action when the rules governing data practices are violated.** The statute should outline basic requirements and prohibitions to protect personal data, which should be further elaborated through rulemaking. Violations of these requirements and prohibitions should be actionable in order to enforce compliance with individuals' privacy rights (no requirement to prove negligence or prove actual damage).
b. **Enforcement by federal and state agencies and a private right of action.** There are other agencies, such as the Federal Communications Commission (FCC), that have specific enforcement duties, and they should coordinate those actions with the U.S. Data Protection Agency, as the FCC and the Federal Trade Commission do on enforcing telemarketing rules.
c. **The ability to seek injunctive relief to stop illegal practices quickly.** It is essential to ensure individuals' personal data are not subject to continued practices that violate their rights.

d. **Meaningful penalties for violations.** Penalties that are seen as merely "the cost of doing business" provide no incentive for compliance. Penalties should have a real impact on companies' bottom lines. For instance, under the General Data Protection Regulation in Europe, fines can up to four percent of companies' total annual worldwide turnover or 20 million Euros, whichever is higher (this is not per violation; it is assessed on the basis of the gravest violation). Contrast this amount with the maximum civil penalty that the Federal Trade Commission (FTC) can obtain, currently $41,484 per violation. Furthermore, the FTC can only seek such penalties in privacy cases when companies have violated a court order or settlements that they have entered into. In other words, they get a free "first bite of the apple" and only face penalties if they continue their bad practices. Individuals and law enforcement agencies should be able to seek penalties, within a specified range, that are appropriate to the circumstances and that give the law real "teeth."
e. **The ability to obtain redress for affected individuals.** If violations result in financial losses or other specific injuries to individuals, enforcement actions should be able to seek appropriate redress such as monetary compensation, correcting inaccurate data, or purging data.
f. **The ability to change companies' data practices going forward.** Individuals and law enforcement agencies should be able to take action to require companies to change their data practices to align with the relevant rules and prevent future violations.

10. State enforcement

a. Maintain state Attorney General authority
    i. *E.g.* S. 583 DATA Privacy Act (Sen. Cortez-Masto): "(b) Enforcement by State attorneys general.— (1) IN GENERAL.— (A) CIVIL ACTIONS.— In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates this Act or a regulation prescribed under this Act, the State, as parens patriae, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to— (i) enjoin that practice; (ii) enforce compliance with this Act or such regulation; (iii) obtain damages, restitution, or other compensation on behalf of residents of the State; (iv) impose a civil penalty in an amount that is not greater than the product of the number of individuals whose information was affected by a violation and $40,000; or (v) obtain such other relief as the court may consider to be appropriate."

11. Private right of action

a. Provide for private right of action
    i. *E.g.* TCPA 47 U.S.C. § 227: "(3) Private right of action—A person or entity may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate court of that State— (A) an action based on a violation of this subsection or the regulations prescribed under this subsection to enjoin such violation, (B) an action to recover for actual monetary loss from such a violation, or to receive $500 in damages for each such violation, whichever is greater, or (C) both such actions."
b. Specify stipulated or liquidated damages. Examples from federal privacy laws:

i. Cable Privacy Act: 47 U.S.C. § 551—"(2) The court may award— (A) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher; (B) punitive damages; and (C) reasonable attorneys' fees and other litigation costs reasonably incurred."
ii. Video Privacy Protection Act (VPPA): 18 U.S.C. § 2710(c)(2) — "The court may award—(A) actual damages but not less than liquidated damages in an amount of $2,500; […]"
iii. Telephone Consumer Protection Act (TCPA): 47 U.S.C. § 227(b)(3) — "A person or entity may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate court of that State— (A) an action based on a violation of this subsection or the regulations prescribed under this subsection to enjoin such violation, (B) an action to recover for actual monetary loss from such a violation, or to receive $500 in damages for each such violation, whichever is greater, or (C) both such actions. If the court finds that the defendant willfully or knowingly violated this subsection or the regulations prescribed under this subsection, the court may, in its discretion, increase the amount of the award to an amount equal to not more than 3 times the amount available under subparagraph (B) of this paragraph."

c. The ability to seek injunctive relief to stop illegal practices quickly. It is essential to ensure individuals' personal data are not subject to continued practices that violate their rights.
d. No requirement to prove negligence or prove actual damage
e. Ban arbitration clauses
f. Add private right of action to COPPA

12. Government Access to Personal Data

a. Requires a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;
b. Requires clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case;
c. Requires that law enforcement provide the individual concerned with prior notice and the opportunity to contest the search;
d. Authorizes the court reviewing the warrant application to modify the order if the scope of records requested is unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden.

13. Effect on Federal and State Law

a. Do not preempt stronger state laws.
b. Suggested language: "Nothing in this Act modifies or otherwise affects, or shall be construed to modify or otherwise affect, any action for damages or the liability of any person under the law of any State or subdivision of a State. Nothing in this Act preempts laws, rules, or other requirements of a State or subdivision of a State that provide more privacy protection than the provisions of this Act, unless compliance with both the requirements of this Act and the requirements of State law is impossible."
c. Examples of strong anti-preemption clauses in federal privacy laws:
    i. Cable Communications Privacy Act: 47 U.S.C. § 551(g)
        1. "Nothing in this subchapter shall be construed to prohibit any State or any franchising authority from enacting or enforcing laws consistent with this section for the protection of subscriber privacy."

ii. Video Privacy Protection Act: 18 U.S.C. § 2710(f)
    1. "The provisions of this section preempt only the provisions of State or local law that require disclosure prohibited by this section."
iii. Gramm-Leach-Bliley Act: 15 U.S.C. § 6807(a)
    1. "This subchapter and the amendments made by this subchapter shall not be construed as superseding, altering, or affecting any statute, regulation, order, or interpretation in effect in any State, except to the extent that such statute, regulation, order, or interpretation is inconsistent with the provisions of this subchapter, and then only to the extent of the inconsistency. (b) For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter and the amendments made by this subchapter…"

Signed,

Campaign for a Commercial-Free Childhood

Center for Digital Democracy

Color of Change

Consumer Action

Consumer Federation of America

Electronic Privacy Information Center

Parent Coalition for Student Privacy

Public Citizen

Privacy Rights Clearinghouse

U.S. PIRG