FAILURES OF THE CURRENT SYSTEM:
The United States Needs a Data Protection Agency

The United States confronts a crisis. Digital giants invade our private lives, spy on our families, and gather our most intimate facts, on a mass scale, for profit. The Federal Trade Commission (FTC) has failed to intervene, consistently failing to enforce its own Consent Orders. The system is broken. Updated privacy laws and a new data protection agency are needed now.

Why does it matter to your constituents?

- The transfer of 87 million user records to Cambridge Analytica could have been avoided if the FTC had enforced its Consent Order with Facebook.
- The FTC has failed to enforce its own orders:
    - The FTC failed to enforce the consent order against Google even after the FTC chair warned that Google's consolidation of Internet services would be bad for consumers
    - The FTC failed to enforce the consent order against Facebook even after repeated violations, including the transfer of user data to Cambridge Analytica, were widely known
- The FTC failed to block mergers that stifled competition and innovation:
    - The FTC approved Google's acquisition of DoubleClick
    - The FTC approved Google's acquisition of Nest
    - The FTC approved Facebook's acquisition of WhatsApp and Instagram
- The FTC has failed to impose fines even when it could. For example, Uber was found twice in violation of a consent order and the FTC imposed no fines.
    - In contrast, EU antitrust authorities fined Facebook $122 million for making false representations, and German competition authorities recently cited privacy concerns to block Facebook's integration of WhatsApp and Instagram user data.
- The Federal Communications Commission (FCC) has also used its fining authority to impose substantial fines on telecommunications companies that violate user privacy. In 2015, the FCC fined AT&T $25m for a data breach. In 2014, the FCC fined Verizon $7.4m to settle a privacy case.
- The FTC has failed to act on dozens of detailed consumer privacy complaints alleging unfair practices concerning data collection, marketing to children, cross-device tracking, consumer profiling, user tracking, discriminatory business practices, and data disclosure to third-parties.
- Over the last decade, because of the FTC's failure to act, the problem has grown dramatically from cookie tracking to ubiquitous, cross-device mass surveillance of individuals and communities.

The United States needs a new approach. While the FTC helps to safeguard consumers and promote competition, it is not a data protection agency. The US needs a federal data protection agency focused on privacy protection, compliance with data protection obligations, and emerging privacy challenges. Federal law must establish a data protection agency with resources, rulemaking authority and effective enforcement powers.

Scope of activities for a U.S. Data Protection Agency

- Assess current threats to data protection in the U.S.
- Promulgate rules to protect the privacy and security of individuals' personal information.
- Ensure that privacy practices and processing are fair, non-discriminatory, and comply with Fair Information Practices.
- 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.
- Examine the social, ethical, and economic impacts of high-risk data processing and propose remedies.
- Ensure fair contract terms in the market, including the prohibition of "pay-for-privacy provisions" and "take-it-or leave it" terms of service.
- Promote privacy innovation, such as privacy by design and data minimization techniques.
- Issue opinions and other forms of guidance on complying with privacy and security obligations and on innovating to address emerging privacy challenges.
- Take complaints and information from the public on data protection matters.
- Make annual reports to the public and Congress on the state of privacy in the United States and issue other reports as appropriate.
- Participate in federal agencies' rulemaking concerning the Privacy Act and other federal privacy laws and in trade negotiations.
- 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.
- Enforce privacy statutes and rules as authorized by Congress, with a broad range of tools including civil penalties, injunctive relief, and equitable remedies.
- Represent the U.S. at international data protection meetings.
- Provide the annual assessment for the Privacy Shield.
- Create and disseminate public education materials.

PREEMPTION IN A FEDERAL PRIVACY BILL:
A Bad Idea for Consumers, Civil Rights, and Innovation.

The states are the "laboratories of democracy," able to respond to emerging privacy challenges and develop innovative solutions. Congress has long respected the critical role of the states in the privacy field. Federal privacy laws, such as the video privacy law (which now provides privacy for Internet streaming services), establish federal baselines that allow the states to develop stronger privacy laws if they choose. And the states have developed important safeguards that protect Americans from identity theft, financial fraud, and cyber attacks by bad actors, foreign and domestic. Federal law that preempts stronger state law would undermine new privacy laws, such as the California Consumer Privacy Act, and leave Americans vulnerable to higher levels of cyber crime.

Why does it matter to your constituents?

According to the Nation Conference of State Legislatures (NCSL), there are hundreds of privacy laws across the United States that help safeguard the privacy and security of Americans. For instance, the NCSL notes that "lawmakers in half the states have enacted laws to prevent employers from requesting passwords to personal Internet accounts to get or keep a job." Close to half of the states considered measures in 2018 to restrict how Internet service providers can collect or disclose consumer data. Every state in the nation has adopted data breach notification laws. Many have also enacted identity theft protections and data disposal rules that protect consumer reports, information derived from consumer reports, and electronic health records.

Federal baselines are particularly important in the information security field: these problems are rapidly changing and the states need the ability to respond as new challenges emerge.

State Attorneys General also play a key role protecting the privacy rights of consumers. The State AGs are on the front lines of privacy protection, working across party lines, to help reduce cyber crime and safeguard personal data. Federal preemption could undermine both existing state privacy and state enforcement efforts.

Some of the model state laws that could be undercut by federal preemption:

- The California Consumer Protection Act - protects personal data
- Illinois Biometric Information Privacy Act - safeguards biometric data
- Vermont Data Broker Act - protects consumers from fraudulent data use
- Massachusetts Data Security Law - establishes strong security standards
- Alaska and Nevada's Genetic Privacy laws – safeguard genetic data
- Michigan Internet Privacy Protection Act – safeguards employee social media privacy
- Florida Information Protection Act - provides timely data breach notification

Federal baseline legislation should ensure a basic level of protection for all individuals in the United States. Federal preemption would place Americans at greater risk of cyber attacks.

HOW DATA IS COLLECTED TODAY:
Disproportionate Harms, Civil Rights Violations, and Impacts on People of Color

Our privacy laws are decades out of date, leaving ample space for bad actors to exploit a lack of civil rights and anti-discrimination protections for disadvantaged groups and for other actors to unintentionally replicate, and in many cases, amplify, the systems of bias that reinforce the racist, social, and economic hierarchies of our society.

Without new legislative protections empowering regulators to stop harmful and discriminatory impacts, we risk undermining decades of civil rights protections.

Why does it matter to your constituents?

New data-gathering techniques, digital advertising, and automated decision-making are increasingly having discriminatory impacts in areas such as housing, employment, health, education, voting rights and lending. Examples of these impacts include:

- Despite the 1968 Fair Housing Act outlawed redlining, data mining models used by mortgage lenders are increasingly replicating the discriminatory impacts of redlining. Researchers found that people of color paid 5.3 basis points extra in interest with online mortgage applications, little different than the 5.6 additional points they paid when applying for mortgage loans in person. Often, it is difficult to discern exactly why these algorithms result in unfair rates because the underwriting is a "black box" where even the programmers are unclear on how the algorithm is making decisions.
- Criminal Justice Risk Assessment tools arm judges with racially biased algorithms to use in handing down sentences. Data shows that the tool disproportionately labels Black people as “high risk” at up to two times the rate of white people with the same types of offenses. The computerized tool brands individuals with risk labels for broad categories of behavior based on data - such as age, gender, what neighborhood they live in - that has nothing to do with their actual risk or danger. The fundamental problem is that the tool doesn’t actually predict the individual’s behavior at all: it predicts law enforcement behavior as to whether the police are likely to arrest that individual again.
- In 2018, Facebook faced an EEOC complaint for discriminatory employment advertisements. According to complaint, businesses bought ads on Facebook to publicize job openings, but targeted them so that no women who use the platform could see them. Additionally, studies have demonstrated gender and employment discrimination through Google ads.
- In 2018, officials and Housing and Urban Development accused Facebook of engaging in housing discrimination. According to the complaint, Facebook permitted advertisers to discriminate based on disability by blocking ads to users the company categorized as having interests in "mobility scooter" or "deaf culture." It similarly discriminated based on familial status by not showing ads to users that were labeled as being interested in "child care" or "parenting," according to the complaint. And in 2017, after Facebook promised to end race-based targeting housing ads, ProPublica demonstrated how dozens of racist housing ads were approved by Facebook within minutes.
- Throughout the 2016 election cycle, Facebook not only underestimated the threat of foreign and domestic election interference and voter suppression, the company repeatedly lied about the extent of the problem and when they become aware of it. A report published by the Senate Intelligence Committee demonstrated that Black users were heavily targeted on the platform during the election cycle in a coordinated campaign to suppress their vote.

To address these numerous, complicated, and growing challenges, it is critical that legislation be brought forward that ensures algorithmic transparency and accountability, is built on a familiar privacy framework, such as the original U.S. Code of Fair Information Practices and the widely followed OECD Privacy Guidelines, and is rooted in existing civil rights laws pertaining to housing, employment, voting rights, public access, and finances.

KIDS ARE VULNERABLE TARGETS IN TODAY'S INTERNET UNIVERSE.
THEY NEED STRONG DATA PRIVACY PROTECTIONS.

The internet business model that treats users' data as a commodity is especially unfair as applied to children. Yet today, with the advent of the smartphone, social media, YouTube, smart devices in the home, and tech in schools, children's data is being collected at all hours of the day and churned into targeted marketing in ways that unscrupulous marketers only dreamt of years ago.

Why are children at risk?

Data collection: kids are vulnerable—yet to develop an understanding of the value of privacy and the impact of their sensitive information being in the hands of others. They have less digital skills, less awareness of privacy risks and how to avoid them. Compromising children's privacy can sometimes endanger their safety.

Marketing: kids are vulnerable—lacking the cognitive capacity to identify advertising, understand its purpose and defend against it. They are easy prey for ads disguised as content, like toy unboxing videos with paid influencers masquerading as friends. Marketers crave kids' data—kids are more easily persuaded, they help drive purchasing in the household, and their preferences formed today can lead to brand loyalty for life.

Why does this matter to your constituents?

- Big Tech incursions on kids' privacy are growing every day, with AI "friends," voice assistants as entertainment hubs for kids, and digital technology now interweaved with education.
- Children's vital social and educational interactions now come with a risk to privacy and little ability for children or parents to opt-out or seek greater privacy protections. We are asking kids and families to give up privacy in exchange for the ability to participate in friendships, school, and their communities.
- Privacy policies are hard to find, vague, and impossible for parents or children to understand, and permit way too much leeway for how companies and their partners can use children's data.
- Children have no or limited capacity to consent to their information being collected and used, so efforts to purportedly obtain their consent are meaningless.
- YouTube, social media, and much of the Internet are designed to profit from children's data, and most sites make little attempt to comply with COPPA or to have special policies which apply to children's data.
- COPPA enforcement by the FTC is completely lacking. The FTC has stood by while Big Tech companies have flouted COPPA by tracking kids on popular websites and apps.
- COPPA is not sufficient. We need more to protect children in the ways they use the internet, apps, and social media today.
- Children's data from internet and app activity is being unfairly used to target them with predatory and manipulative marketing, which is harmful to their healthy development.

Data privacy protections should include:

- Strong limits on collection, use, and disclosure of children's and teens' information, broad definitions of sensitive information protected, including data that reveal sensitive personal information, and narrow definitions of excepted internal purposes.
- Unique children's privacy policies employed on all sites and platforms used by children.
- Proper protection and encryption of kids' data, and deletion of all data legally collected when no longer needed for operational purposes, or sooner at the request of parents.

- A prohibition on targeted marketing to children and teens under the age of 17.
- Creation of a privacy protection agency with true enforcement powers and resources dedicated to the unique concerns of children, which can evolve and keep abreast of changing tech and business practices.
- Rules requiring transparency in all practices, prominent privacy policies written in plain English, and detailed information about types of information collected before parental consent is requested.

ENFORCEMENT FOR PRIVACY LEGISLATION

A comprehensive law to protect privacy in the United States will only be effective if it provides for robust enforcement. The law should include:

- 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, regardless of whether they have suffered financial or other tangible "harm."

- Enforcement by federal and state agencies and a private right of action. Data protection is a broad mandate and responsibility for enforcing individuals' rights cannot be placed on one entity alone. The United States should have a data protection agency, as many other countries in the world do, to promulgate rules, issue guidance, educate the public, and take enforcement 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 data protection agency, as the FCC and the Federal Trade Commission do on enforcing telemarketing rules. State attorneys general and individuals must also have the ability to enforce federal privacy law, as is the case with telemarketing.

- 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.

- 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."

- 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.

- 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.

ENFORCE FAIR INFORMATION PRACTICES AND SET OTHER DATA USE LIMITS THAT AIM TO ACHIEVE FAIR AND JUST OUTCOMES

Today our lives are shaped by unencumbered and ubiquitous commercial surveillance: we live in a world of unfettered data collection, of unrestrained data uses, and unlimited data sharing and hording. More and more of our experiences and life chances are determined by automated decisions based on predictive and classifying analytics. These decisions are based on data about us – our behaviors and characteristics. They are made by companies to advance their interests. These systems tend to track us across time, space and markets, and classify us as "winners" and "losers." Without laws that limit how companies can collect, use, share and accrue this data, we end up with an information and power asymmetry benefitting companies rather than consumers. Individual, group or societal interests are diminished and our privacy and other basic rights and freedoms are at risk.

Why does it matter to your constituents?

Without effective safeguards, our rights to privacy, self-determination and autonomy are at risk, and many other associated rights and freedoms are undermined: our freedom from manipulation, intrusion and surveillance; the right to dignity; the right to fair processing of our data; and the right to equal opportunity, freedom of information, and freedom of speech. This power imbalance also affects individuals' right to be free from profiling and unjust discrimination. Vulnerable populations are particularly susceptible to exploitation and harm. Individuals may suffer from financial, reputational, or psychological effects. Societal harms include increasing inequality, the chilling of speech, the undermining of public trust in corporate entities, public institutions and the democratic process, increasing conformity and ideological polarization, and unsustainable consumption and negative environmental impacts.

The scoring of consumers and citizens is ubiquitous and likely to serve only those already advantaged. Consumers and citizens are scored, ranked, described or otherwise classified so that companies, governments and other entities can more easily make decisions about them. These scores are typically driven by the desire to maximize the value to a company's bottom line or to minimize risk (as defined by the organization). This "actuarial logic" is particularly harmful and concerning when applied to what scholars have described as "modern eligibility" determinations, including for identity verification, fraud assessment, credit, job applicants' likelihood of success. These data uses are especially worrisome as they appear to replicate and even amplify racial, social and economic inequities.

Location-based tracking and advertising is inescapable, and harms are manifold. Many mobile apps and mobile operating systems, as well as phone companies and automakers, for example, track users' movements. This information is used for hyper-personalized and location-based advertising, or predatory marketing. Examples include:

- location information used to target emergency-room visitors with ads for personal injury lawyers;
- Pay-day loan targeting;
- Communities of color targeted with fast food advertising with devastating effects on public health;
- Location information used to determine risk and to set car insurance rates;
- The Massachusetts Attorney General settled a case involving geofencing around women's reproductive healthcare facilities. An advertiser had tracked consumers' location and targeted them with ads for

pregnancy counseling and adoption agencies seemingly aimed at persuading pregnant women not to proceed with an abortion.

Because of the opacity of industry's data practices, many objectionable uses often don't come to light, and their harms are difficult to assess.

Personalized price steering and price discrimination and other manipulative data practices on e-commerce sites are numerous and are applied without our knowledge. For example, we can be manipulated in the way in which products are shown (price steering), or by customizing the prices of products (price discrimination). Lack of transparency around data practices and reduced marketplace competition all work to disadvantage consumers and to undermine their autonomy.

Examples of corporate wrongdoing:

- With the acquisition of the Wi-Fi router company Eero, Amazon is one step closer to the complete take-over of our homes. Amazon's Echo and its virtual assistant Alexa have turned the home into a place where every corner, from smart microwaves to wall clocks, washing machines, televisions, the nursery and the bedroom are placed under surveillance.
- Google deceptively markets the apps in its "Family" section of the Google Play Store as safe for children, but the apps often violate the Children's Online Privacy Protection Act (COPPA). Google also makes substantial profits collecting many types of personal information from children on YouTube, including geolocation, unique device identifiers, mobile telephone numbers, and persistent identifiers used to recognize a user over time and across different websites or online services. Google collects this information without first providing direct notice to parents and obtaining their consent, as required by COPPA, and Google uses it to target advertisements to kids across the internet, including across devices.
- In 2018, Facebook admitted to the unlawful transfer of 87 million user profiles to the data analytics firm Cambridge Analytica, which harvested the data without user consent. Cambridge Analytica specializes in "psychographic" profiling, which uses data collected online to identify personalities of voters and influence voter behavior through targeted advertising. The firm sought to suppress Black voters and other liberal-associated demographic groups during the 2016 election.

To even out the power and information imbalance between powerful companies and individuals, baseline federal legislation must at a minimum incorporate an established privacy framework, such as the U.S. Code of Fair Information Practices (FIPs) and the OECD Privacy Guidelines. These frameworks create obligations for companies that collect data and rights for individuals. The goal of these principles is to protect individual privacy by placing limits on what companies can know about us. Core principles include:

- Transparency of business practices
- Data collection and use limitations
- Data minimization and deletion
- Purpose specification
- Access and correction rights
- Accountability
- Data accuracy
- Confidentiality/security

While FIPS focus on data and the conditions under which data must be processed, their ultimate goal is to address the information and power imbalance between individuals and entities with large amounts of data about them. While FIPs will not solve all of today's information society's challenges, they are a necessary condition for creating a level playing field between individual, group and societal interests on the one hand and companies' interests on the other.

LAW ENFORCEMENT ACCESS TO PERSONAL DATA

Federal privacy laws typically limit the disclosure of personal information to third parties, including law enforcement agencies. Congress should enact a statutory standard that reflects Fourth Amendment interests and recognizes the legitimate basis for government access to personal data stored by private companies. This is all the more important after the Supreme Court's recent decision in the *Carpenter* case,[1] which established that individuals have a Constitutional interest in their personal data held by third parties.

Federal privacy law should include clear limits on government access to personal data:

- Require a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order;
- Require 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;
- Require that law enforcement provide the individual concerned with prior notice and the opportunity to contest the search;
- Authorize 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.

Why does it matter to your constituents?

Federal privacy laws, such as the video privacy law and the cable privacy law, provide important protections against misuse of certain personal data by both businesses and government agencies. The failure to establish broader limitations on access by government agencies leaves consumers at risk of dragnet investigations and leaves companies subject to litigation for violating fiduciary obligations. These provisions are also important to ensure that personal data of Europeans can be lawfully collected by U.S. companies. In the annual "Privacy Shield" review, the European Commission considers whether U.S. law permits mass surveillance that would be impermissible in Europe. Without rules limiting disclosure of personal data to particularized investigations, transatlantic data flows could be suspended, at a huge cost to the U.S. economy.

After the Supreme Court's recent decision in *Carpenter* Congress should establish clear rules for access to personal data by law enforcement agencies. Both Justice Sonya Sotomayor and Justice Samuel Alito have written that Congress should help clarify and define the scope of privacy rights even after the Supreme Court has ruled.

[1] EPIC, *Carpenter v. United States*, https://epic.org/amicus/location/carpenter/

ESTABLISHING ALGORITHMIC GOVERNANCE TO ADVANCE FAIR AND JUST DATA PRACTICES

The use of secret algorithms based on individual data permeates our lives. Concerns about the fairness of automated decision-making are mounting as artificial intelligence is used to determine eligibility for jobs, housing, credit, insurance, and other life necessities. Bias and discrimination are often embedded in these systems yet there is no accountability for their impact. All individuals should have the right to know the basis of an automated decision that concerns them. And there must be independent accountability for automated decisions.

Why does it matter to your constituents?

Without knowledge of the factors that provide the basis for decisions, it is impossible to know whether government and companies engage in practices that are deceptive, discriminatory, or unethical. The Pew Research Center recently found that most Americans are opposed to algorithms making decisions with consequences for humans, and 58% think algorithms reflect human bias. Examples of algorithmic errors that have recently been uncovered include:

- Amazon was forced to abandon its artificial intelligence-based recruiting tool after discovering that, based on the data it had "learned" from, it preferred male candidates.
- A Google image matching algorithm identified people of color as "gorillas."
- Facial recognition software was 34% less accurate for dark-skinned woman than for white men.
- Amazon, Verizon, UPS excluded older workers from job opportunities with ads on Facebook.
- In 2017, Facebook pledged to change its advertising procedures to prevent rental companies from discriminating against tenants based on race, disability, gender, and other characteristics. However, Facebook was sued in 2018 for allegedly still allowing the practice.

Additionally, protecting algorithms as a trade secret creates a barrier to due process. Trade secret protected algorithms are very likely to reinforce existing prejudices and inequalities through a "techno-social divide" and act as a barrier to information, which fundamentally impacts human rights and social justice.

Algorithmic transparency, to advance fair and just outcomes, is now a core element of modern privacy law and should be included in U.S. privacy law. There must be:

- **Transparency:** Data inputs and algorithms be made available to the public.
- **Accountability:** Entities that improperly use data or algorithms for profiling or discrimination should be held accountable, particularly for misuse of data concerning vulnerable populations. Individuals should have legal remedies for unfair decisions. They should be able to easily access and correct inaccurate information about them.
- **Oversight:** Independent mechanisms should be put in place to assure the integrity of the data and the algorithms that analyze the data. These mechanisms should help ensure the accuracy and the fairness of the decision-making.

We urge you to implement the Universal Guidelines for Artificial Intelligence [https://thepublicvoice.org/ai-universal-guidelines/], the first human rights framework for AI in U.S. law. The Guidelines maximize the benefits of AI, minimize the risk, and ensure the protection of human rights.