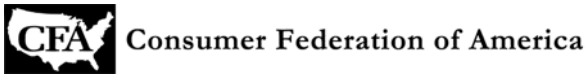
Privacy And Digital Rights For All

A blueprint for the next Administration



Introduction

We are a coalition of leading privacy, civil rights, and consumer organizations that have come together to develop a policy framework for protecting the privacy of all people in the United States. We are particularly concerned about protecting the most vulnerable segments in our society, including Black and Brown communities, children, and low-income populations. We are advocating for federal baseline privacy legislation and action by government agencies to protect individuals from discriminatory data processing practices and to ensure their privacy rights.

The United States is facing an unprecedented privacy and data justice crisis. We live in a world of constant data collection where companies track our every movement, monitor our most intimate and personal relationships, and create detailed, granular profiles on us. Those profiles are shared widely and used to predict and influence our future behaviors, including what we buy and how we vote. Through a vast, opaque system of algorithms and other automated decision-making processes, we are sorted into categories based on data about our health, finances, location, gender, and race.

The impacts of this commercial surveillance system are particularly harmful for communities of color and low-income populations, fostering discrimination in employment, government services, healthcare, education, and many other institutions. In the absence of civil rights and anti-discrimination protections for the digital marketplace, Big Data systems can produce disparate outcomes exacerbating existing hierarchies and inequities in our society.

Children and teens require special attention from policymakers. While there are some existing government privacy protections for the youngest children, the explosive growth of the online digital marketplace has made young people of all ages vulnerable to an onslaught of aggressive marketing and data collection practices that require additional safeguards.

Without laws that limit how companies can collect, use, and share personal data, we end up with an information and power asymmetry that harms consumers and society at large. Individual, group and societal interests are diminished, and our privacy and other basic rights and freedoms are at risk.

We urgently need a new approach to privacy and data protection. The time is now.

The U.S. public strongly supports new laws that will protect privacy and digital rights. Recent polling from the Pew Research Center found that 3 out of 4 Americans believe there should be more government regulation of what companies do with their data. In another poll from Morning Consult, 79 percent of respondents agreed that Congress should craft a bill that improves their privacy rights. In the face of rising concerns over the harmful data practices of the technology industry, this Congress has made progress towards crafting effective federal privacy legislation, with bipartisan agreement on the need for a federal privacy bill.

The COVID-19 pandemic has highlighted the need for a comprehensive baseline U.S. privacy law. Technology companies, remote-learning providers, and employers are taking advantage of the pandemic to collect troves of personal data. We need presidential leadership to address these challenges.

While some solutions are legislative, we encourage the Administration to prioritize and act swiftly to put in place privacy and data justice protections: affirming privacy, surveillance, and corporate concentration issues as critical racial justice issues; ending the surveillance of Black and Brown communities; protecting the privacy of federal employees; eliminating bias and disparate impacts in government programs by requiring the federal government and companies with federal contracts to follow exemplary privacy and data justice practices; encouraging robust and meaningful agency enforcement; and supporting action in Congress to enact effective privacy laws. To that end, we urge you to adopt the following ten action items starting next year. We are available to assist in drafting any orders, memos, and policies mentioned below.

Please note: A broad group of leading privacy, consumer and civil rights organizations produced this memorandum to underscore the importance of bold action in digital rights and privacy. Because the organizations involved and the issues addressed are diverse, not every organization works on or endorses each item listed, although all firmly support the vast majority. The organizations are unanimous in their support for pro-consumer and pro-citizen action on these issues.

Action 1: Recognize Privacy and Surveillance as Racial Justice Issues, and Enact Meaningful Changes to Protect Black and Brown Communities

Recommendations for Day One

- Send a memorandum across the Administration reiterating the need for privacy protection that specifically addresses racial justice. This memo should urge the Department of Justice (DOJ) to promulgate guidance that Title VI of the Civil Rights Act of 1964 prohibits discriminatory data processing practices in determinations about federal financial assistance.

Recommendations for First 100 Days

- Require impact assessments from agencies about the use of algorithms and other automated processes in federally financed programs, including outsourced data processing, impact assessments of disparate impacts caused by these processes, and plans to eliminate those disparate impacts.

- Direct all agencies with civil rights authorities to evaluate discriminatory processing of personal data in their jurisdictions, engage in rulemaking or enforcement actions to eliminate discriminatory processing of personal data, and make legislative recommendations if additional authorities are necessary. This includes but is not limited to the Department of Justice, Department of Housing and Urban Development, Equal Employment Opportunity Commission, Consumer Financial Protection Bureau, Food and Drug Administration, Federal Trade Commission, Department of Homeland Security, Department of Health and Human Services, Department of Labor, Department of Agriculture, and Department of Education.

- Direct agencies not to adopt the use of algorithms or other predictive models as a safe harbor or defense against disparate impact claims or other claims that prohibit racial discrimination.

- Establish an Interagency Task Force on Data Privacy and Justice, with participation from the FTC, DOJ, and other relevant agencies with the goal of developing tools to identify and eliminate data practices with disparate impact.

Action 2: Establish Algorithmic Governance and Accountability to Advance Fair and Just Data Practices

Recommendations for First 100 Days

- Establish a National Algorithmic Accountability Initiative to investigate how new data-gathering techniques, digital advertising, and automated decision-making may have discriminatory or disparate impacts in areas such as housing, employment, health, education, voting rights, and lending.
- Task the Initiative with producing recommendations for legislative and regulatory principles, to be adopted in federal privacy legislation.
- Ensure an open and inclusive process for U.S. policy on AI.
- Require that any AI system adopted by an agency be supported by a valid public purpose, thoroughly vetted, and backed by accountability measures that allow a person unduly harmed by the system to obtain redress.

Recommendations for Year One

- Require law enforcement and intelligence agencies to conduct algorithmic impact assessments for their use of automated systems.
- Urge the Securities and Exchange Commission (SEC) to require public companies to disclose in their shareholder disclosures how the company processes personal data, including algorithmic processing.

Recommendations for Legislative Action

- Promote federal privacy legislation that requires algorithmic accountability (including impact assessments); incorporates the principles of transparency, accountability, and oversight; and establishes criteria for permissible automated decision-making processes.
- Promote legislation based on the Universal Guidelines for Artificial Intelligence, the first human rights framework for AI in U.S. law, and the OECD AI Principles as a baseline for AI regulation.

See more recommendations for establishing algorithmic governance here.

Action 3: Promote Privacy Protections and Encourage Enactment of a Baseline Comprehensive Federal Privacy Law

Recommendations for First 100 Days

- Appoint a White House Data Privacy and Justice czar.
- Issue an executive order to protect federal employees from inappropriate data collection, consistent with the Privacy Act of 1974.
- Issue an executive order to restrict government contracts to companies that protect privacy, consistent with the Privacy Act of 1974.
- Ensure that any trade negotiation or prospective outcome on digital trade talks must prioritize consumer protections and rights, e.g. by protecting people's privacy rights and personal data protection, and ensuring algorithmic transparency and accountability.
- Ensure that individuals' personal data coming into the U.S. from abroad, as well as data about those in the U.S. being processed abroad, receives protections that reflect highest global civil liberties and privacy standards.

Recommendations for Legislative Action

- Urge Congress to pass federal privacy legislation. This legislation should:
    - Restrict the collection, use, storage, and transfer of data to permissible purposes (rather than including 'opt in' or 'opt out' consent models).
    - Ensure civil rights protections, algorithmic accountability, and safeguards for fairness and equity online.
    - Prohibit "take it or leave it" terms.
    - Guarantee a private right of action so individuals can enforce their rights and corporations can be held accountable.
    - Establish a federal floor for privacy protection, not a ceiling.
- Encourage Congressional ratification of the Council of Europe Convention 108+. This convention supports innovation and user privacy rights and is the only binding international treaty on data flows and personal data protection.

Action 4: Establish a Data Protection Agency

Many democratic nations have a dedicated data protection agency with independent authority and enforcement capabilities. While the FTC helps to safeguard consumers and promote competition, it is not a data protection agency. The FTC lacks rulemaking authority on privacy. Furthermore, the agency has failed to enforce the orders it has obtained. The US needs a federal agency focused on privacy protection, compliance with data protection obligations, and emerging privacy challenges. The agency should also examine the social, ethical, and economic impacts of high-risk data processing and oversee impact-assessment obligations.

Recommendations for First 100 Days

- Establish a White House Task Force on how to bring data, privacy, and digital rights work under one roof leading up to, during, and after the establishment of a data protection agency.

Recommendations for Legislative Action

Urge Congress to establish a data protection agency, with the adequate resources, rulemaking authority and enforcement powers to:

- Promulgate rules to protect the privacy and security of individuals' personal information;
- Ensure fair contract terms in the market, including by prohibiting "pay-for-privacy provisions" and "take-it-or leave it" terms of service;
- Examine the social, ethical, and economic impacts of high-risk data processing and oversee impact-assessment obligations;
- Require meaningful changes in business practices and issue penalties in response to violations; and
- Cooperate with other agencies on overlapping issues such as antitrust, consumer protection, and civil rights.

See more on the need for and uses of a data protection agency here.

Action 5: Ensure Robust Enforcement from the FTC and FCC

Recommendations for Year One

Encourage the FTC and the Federal Communications Commission (FCC) to:

- Make clear that they will take appropriate action under their existing authority to enforce compliance with individuals' privacy rights, recognizing that violations of those rights constitute consumer harm.
- Apply meaningful penalties that have a real impact on noncompliant companies' bottom lines.
- Require meaningful changes in business practices in response to violations.
- Commission 6(b) studies to identify discriminatory processing of personal data in products and services aimed at children, in the ad tech and ed tech industries, in communications, in direct-to-consumer DNA testing, and in other areas over which they have jurisdiction.
- Use their authority to the fullest extent possible to promulgate rules that define unfair and deceptive trade practices, regulate the data practices of companies such as smart grid providers and auto manufacturers, and can result in penalties for first-time violations, if appropriate.

See more on recommendations for stronger enforcement here.

Action 6: Bring Consumer, Privacy, and Civil Rights Experts into Key Government Positions

Recommendations for First 100 Days

Ensure that the people who are selected for positions that involve the technology industry, data, privacy, and digital rights (including but not limited to the DOJ, FTC, FCC, and aforementioned data protection agency) exemplify the following characteristics:

- Be representative of the country, with diversity in race, gender, orientation, and disability;
- Have demonstrated a commitment to civil rights, privacy, and racial justice both online and off;
- Have demonstrated a fluency in digital rights, data, and technology issues, as well as the problems of disparate impact and algorithmic discrimination; and
- Do not have significant conflicts of interest. The Office of Government Ethics should be given the authority to conduct a screening process and recommend against proposed appointees for senior level positions if their employment backgrounds and/or current private sector activities would give rise to potential conflicts of interest requiring recusal.

Action 7: Limit Government Surveillance and Access to Personal Data

Recommendations for Day One

- Ban or place a moratorium on facial recognition and other biometric surveillance by federal authorities.
- Improve oversight and reporting requirements for location data surveillance.
- Immediately stop disproportionate federal government collection, use, storage, and surveillance of personally identifiable information.

Recommendations for Legislative Action

- Promote federal privacy legislation (discussed earlier in this memo) that includes clear limits on government access to personal data, including requirements for:
    - A warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, a grand jury subpoena, or a court order to obtain personal data;
    - 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; and
    - Providing prior notice to the individual concerned, with reasonable exceptions, and the ability of individuals to contest the data request.
- Reform U.S. surveillance laws in response to the European Court of Justice's decision invalidating the EU-U.S. Privacy Shield agreement, including ending bulk collection conducted under EO 12333 and expanding the role of the FISA court in overseeing surveillance under EO 12333 and Section 702.

See more recommended principles for protecting citizens' data from inappropriate law enforcement access here.

Action 8: Protect Children and Teens from Corporate Surveillance and Exploitative Marketing Practices

Recommendations for First 100 Days

- Urge the FTC to begin 6(b) studies on ad tech and ed tech companies' data practices and their impacts on children and teens before undertaking any rulemaking under the Children's Online Privacy Protection Act (COPPA).
- Protect students through an executive order that requires the Department of Education (DoE) to:
    - Prohibit the selling or licensing of student data;
    - Issue recommendations on transparency and governance of algorithms used in education; and
    - Minimize data collection on students, ensure parental consent is affirmatively obtained before disclosing student data, and issue rules enabling parents to access and also govern data on their child.

Recommendations for Legislative Action

- Ensure children and teen privacy is legislatively protected as part of a comprehensive baseline federal privacy bill that:
    - Establishes the special status of children and teens as vulnerable online users; provides strong limits on collection, use, and disclosure of data, and narrowly defines permissible uses;
    - Requires employing privacy policies specific to children's data on all sites and platforms used by children; and
    - Prohibits targeted marketing to children and teens under the age of 18 and profiling them for commercial purposes.
- Strengthen COPPA by raising the covered age to 17 years and under, banning behavioral and targeted ads, banning the use of student data for advertising, and requiring manufacturers and operators of connected devices and software to prominently display a privacy dashboard detailing how information on children and teens is collected, transmitted, retained, used, and protected.

See more recommended principles for protection of children and teens here.

Action 9: Ensure Antitrust Authorities Take Privacy, Digital Rights, and Civil Rights into Account in Merger Review Process

Recommendations for First 100 Days

- In the memorandum about digital rights, privacy, and racial justice that is called for in Action 1, affirm that corporate concentration is also a racial justice issue that should be prioritized, along with privacy issues, in antitrust enforcement.
- Develop an integrated policy and enforcement approach within and among relevant agencies to address competition, privacy, digital rights, and civil rights issues.
- Direct antitrust enforcers to consider privacy and data protection in merger reviews.

Recommendations for Legislative Action

- Encourage Congress to address digital rights and antitrust reforms to prevent corporate concentration among Big Tech companies.

Action 10: Protect Americans' Health Data

Recommendations for First 100 Days

- The executive branch, independent agencies and Congress should review the impact of federal policies regarding digital technologies in health, including current data collection, the use of analytics, data storage, and data transfer practices at the consumer and provider level. For example:
    - HHS should assess how well the Health Insurance Privacy Protection Act (HIPAA) protects the confidentiality and privacy of individuals' health data and identify gaps in protection.
    - HHS should also assess the privacy impact of its policies for sharing patient electronic health records.
    - The FDA should assess its policies for digital medical and non-medical devices.
    - The U.S. Centers for Medicare & Medicaid Services should assess its policies concerning distance healthcare, HIPAA and other existing law pertaining to patient data, current data collection, use (including analytics), storage, and transfer practices at the consumer and provider level.
    - Recommendations on revisions of HIPAA, as well as in federal privacy legislation to maximize protections for patients/health consumers amidst rapidly developing technologies.
- Develop proposals at all levels of government to limit the use of personal data to make health-related inferences and to maximize privacy protections for patients and health consumers.
- Provide guidance and recommendations for federal, state, and local agencies on appropriate use of individuals' personal data to combat the COVID-19 pandemic.
- Protect workers' health-related data from inappropriate access and use as the "workplace" expands into the home and to employees' personal lives.