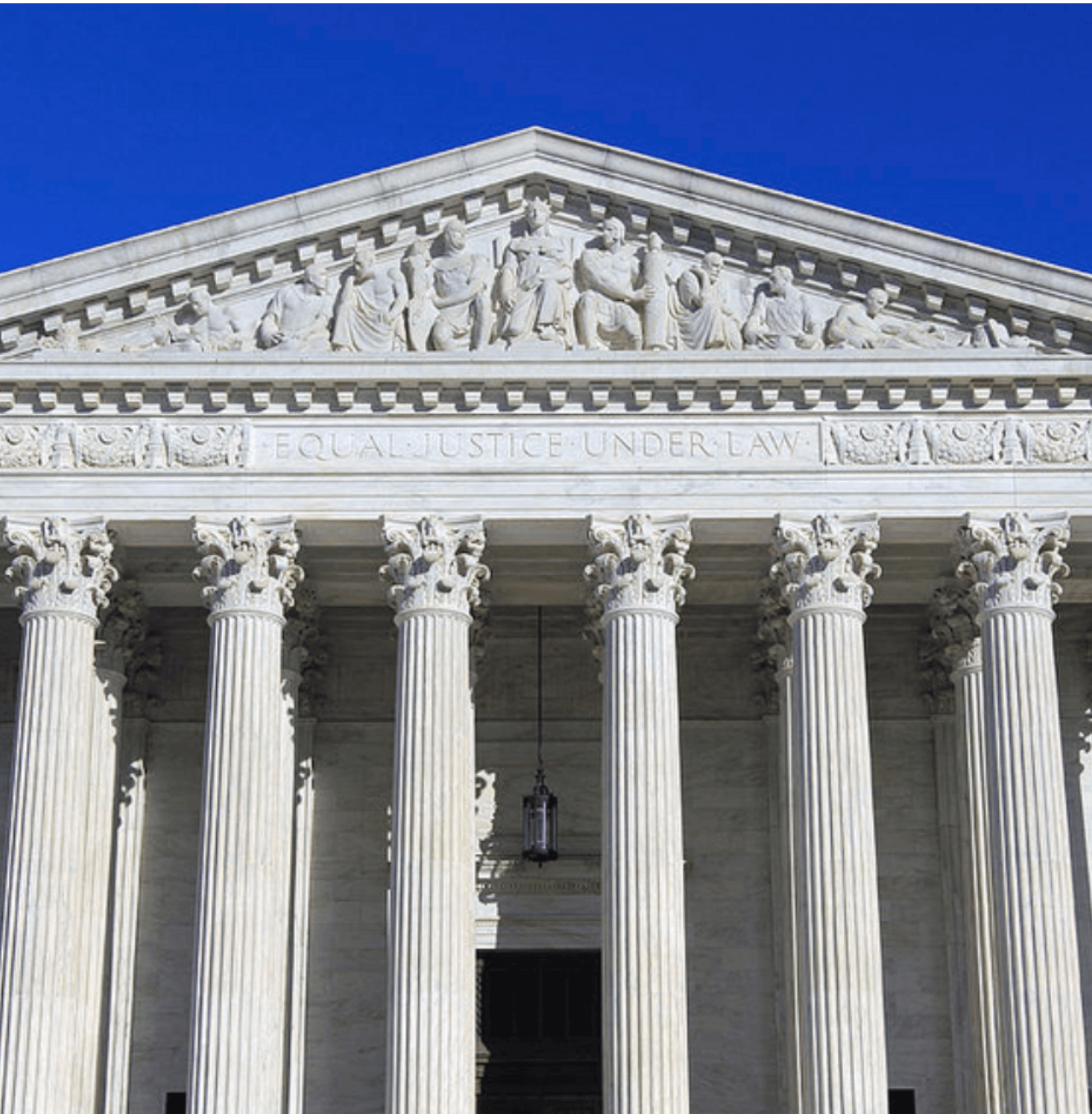
Civil Rights, Privacy, and Technology

Recommended 2021 Oversight Priorities for the 117th Congress



Civil Rights, Privacy, and Technology

In October 2020, more than two dozen of the nation's leading civil rights organizations issued revised **Civil Rights Principles for the Era of Big Data**, building on years of work together on these issues. These principles are designed to ensure that technology serves to provide greater safety, economic opportunity, and convenience to all, not exacerbate disparities in our society or undermine civil rights.

The 2020 principles call for:

1. Ending high-tech profiling;
2. Ensuring justice in automated decisions;
3. Preserving constitutional principles;
4. Ensuring that technology serves people historically subject to discrimination;
5. Defining responsible use of personal information and enhancing individual rights; and
6. Making systems transparent and accountable.

The threats technology (and its misapplication) can pose to civil rights and justice have only grown. The need for these principles — and legislation enshrining them in law — is greater than ever, and the shameful attack on our Capitol and democracy makes the stakes painfully clear. Targeted dis- and misinformation campaigns on social media have aimed to suppress voting, mislead about the census, undermine confidence in our election process, and incite violence and harassment, especially against people of color and other marginalized communities. A variety of invasive surveillance technologies, such as facial recognition and cell phone location tracking, are being used to end-run longstanding civil rights protections for due process and suppress constitutional rights to protest. And tech companies' unchecked collection and use of data exposes underrepresented communities to increased risks of discrimination and predatory targeting.

In recent years, Congress has used its oversight powers to highlight the discriminatory impacts of technology, enforce relevant civil rights protections, reduce disparate impacts, and build a strong evidence base to guide reform and accountability efforts. Moving forward, however, far more significant, sustained, and effective oversight action is necessary, especially as Congress moves to update existing protections and establish modern rules for these technologies. While these legislative reforms are underway, Congress should ensure oversight activities use existing authorities to protect civil rights and promote justice. This work is essential to protecting our democracy. And as the nation continues to navigate the COVID-19 crisis, addressing these questions is vital in promoting a just, inclusive economic recovery.

The 117th Congress must take action to ensure that technology serves all people in the United States, rather than facilitating discrimination or reinforcing existing inequities.

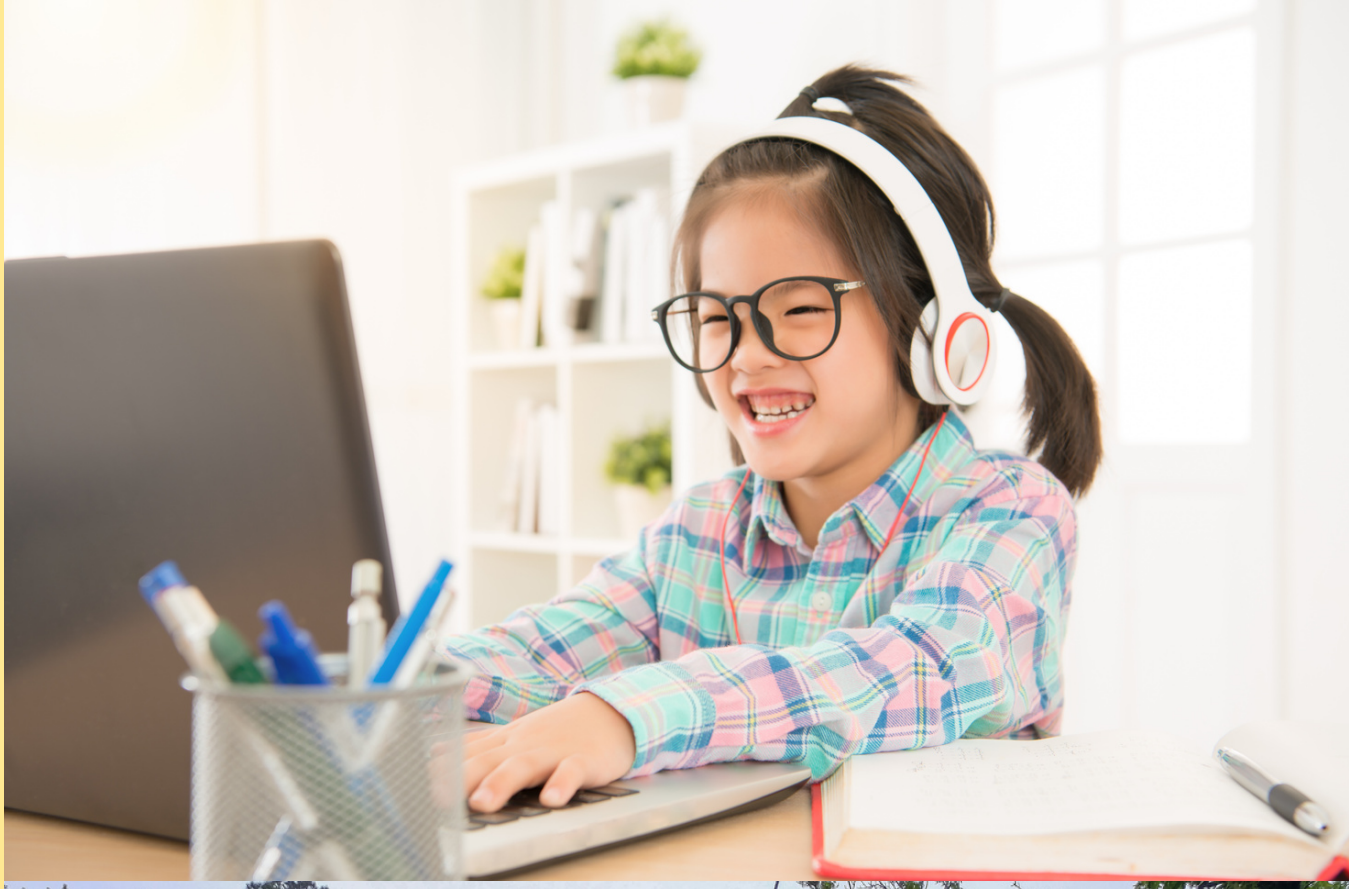
We, the undersigned 14 public interest organizations, have developed this potential oversight agenda to help guide Congress in achieving that mission.

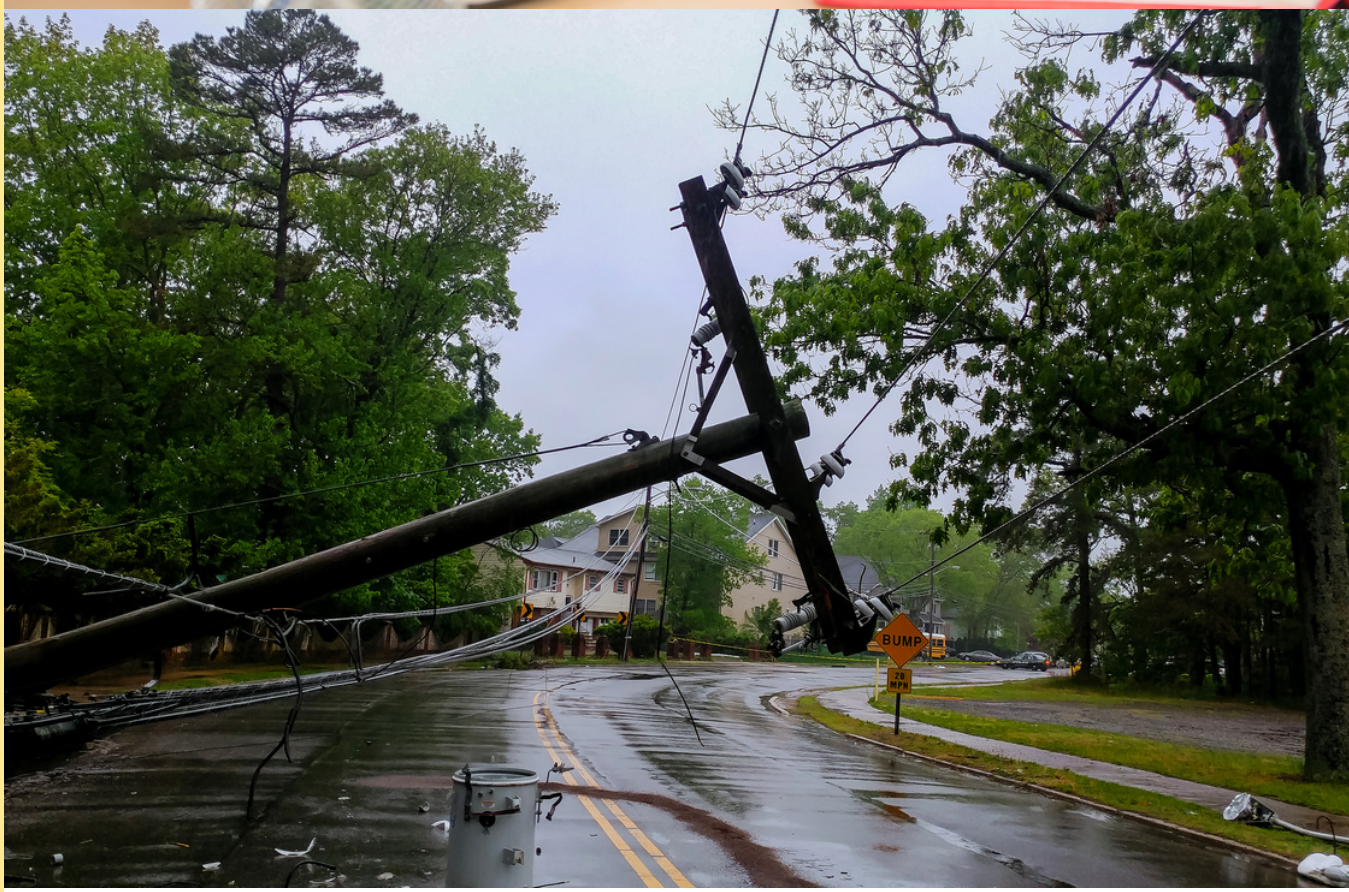
While the priorities laid out here do not reflect the full agenda of all undersigned organizations, and they should be read to complement legislative work to address these challenges, they represent high priority areas of concern for many organizations recommending this agenda. We believe that these goals can and should be accomplished in 2021, and we are excited to collaborate with you on these efforts on behalf of the communities and principles we represent.

Oversight Priorities Signatories

- Brennan Center for Justice
- Center for Democracy and Technology
- Center on Privacy and Technology at Georgetown Law
- Demand Progress Education Fund
- The Leadership Conference on Civil and Human Rights
- The Leadership Conference Education Fund
- Movement Alliance Project
- NAACP Legal Defense and Education Fund
- National Hispanic Media Coalition
- New America's Open Technology Institute
- Public Knowledge
- Ranking Digital Rights
- UnidosUS
- Upturn

Contents





Broadband Internet

Broadband Internet

Overview

Home broadband internet is a prerequisite to participation in modern society. Especially in the face of COVID-19, the internet is a vital tool in finding (and performing) jobs, learning remotely, and staying connected to community. It is also vital to exercising democratic rights; organizing protests against police violence and systemic racism, keeping up with election news, and discussing political priorities all frequently happen online. In the era of COVID-19, these needs are clearer than ever before.

Despite broadband's necessity, tens of millions of Americans lack it, and these gaps occur disproportionately for people of color and people with low incomes. High prices are often the largest barrier. In urban areas, the struggle to get reliable or affordable internet service **more sharply affects** people of color. And according to the **Census Bureau,** barely over half of Native Americans living on tribal lands who have a computer have access to high-speed internet. With communities of color and American Indians disproportionately dying from COVID-19 and disproportionately on the wrong side of the digital divide, our effort must be purposeful in addressing the real-time and future needs of these communities.

Even getting an accurate picture of the state of play is difficult, however. The Federal Communications Commission's mapping process is riddled with loopholes that allow internet service providers to overstate the coverage. As a result, official data systematically underestimates the size of the digital divide.

Congress must take legislative action to close these gaps and guarantee all people in the United States can afford home broadband. Congress must also use its oversight powers to ensure existing programs and stakeholders are fulfilling their obligations and working as effectively as they can. Programs such as Lifeline are falling short of their potential to help people with low incomes get and stay connected, and FCC inaction has allowed internet service providers to fall short of their obligations to provide service on a nondiscriminatory basis.

Broadband Internet

Recommended Oversight Priorities for the 117th Congress

Affordable Broadband

1. Conduct ongoing, robust oversight of the FCC to ensure it is promoting universal affordable broadband by:

- Improving data collection, including by collecting cost/pricing information, making additional details available to researchers, and continuing efforts to collect more detailed information about coverage areas.

- Promoting consumer choice by developing standardized disclosures for price and service.

- Emphasizing effective competition in merger review and regulatory decision-making.

- Ending harmful efforts to undermine the Lifeline program and moving to strengthen the program and its participation rate.

- Prioritizing improvements to broadband access and adoption on tribal lands, including through better consultation procedures.

2. Demand detailed information from the FCC on its efforts to improve takeup of Lifeline and ensure all eligible participants register and receive benefits.

3. Pursue oversight opportunities that complement legislative efforts to legalize municipal broadband networks and preempt state laws that restrict local choice.

4. Demand the FCC ensure deployment and access on tribal lands be a central element in the commission's annual 706 report and report clearly on the extent to which advanced telecommunications capability is being deployed in a reasonable and timely fashion.

Disaster Recovery

5. Demand information from the FCC and major ISPs about their disaster response and network interruption procedures with a focus on recent disasters such as Hurricane Maria in Puerto Rico and the California wildfires. This demand for information should include additional data collection about network status during and after disasters by ensuring the FCC requires ISPs submit this data.

6. Hold a hearing about telecommunications disruptions in the wake of natural disasters, including both major ISPs and organizations representing impacted communities.

Broadband Internet
Recommended Oversight Priorities for the 117th Congress

COVID-19 Response

7. Convene a hearing on COVID-19 and the digital divide, highlighting impacts, federal actions taken to mitigate the divide, and needs moving forward. This oversight work should support legislative efforts to increase affordability by preventing disconnections and maintaining a subsidy for low-income families and others.

Wi-Fi and Unlicensed Spectrum

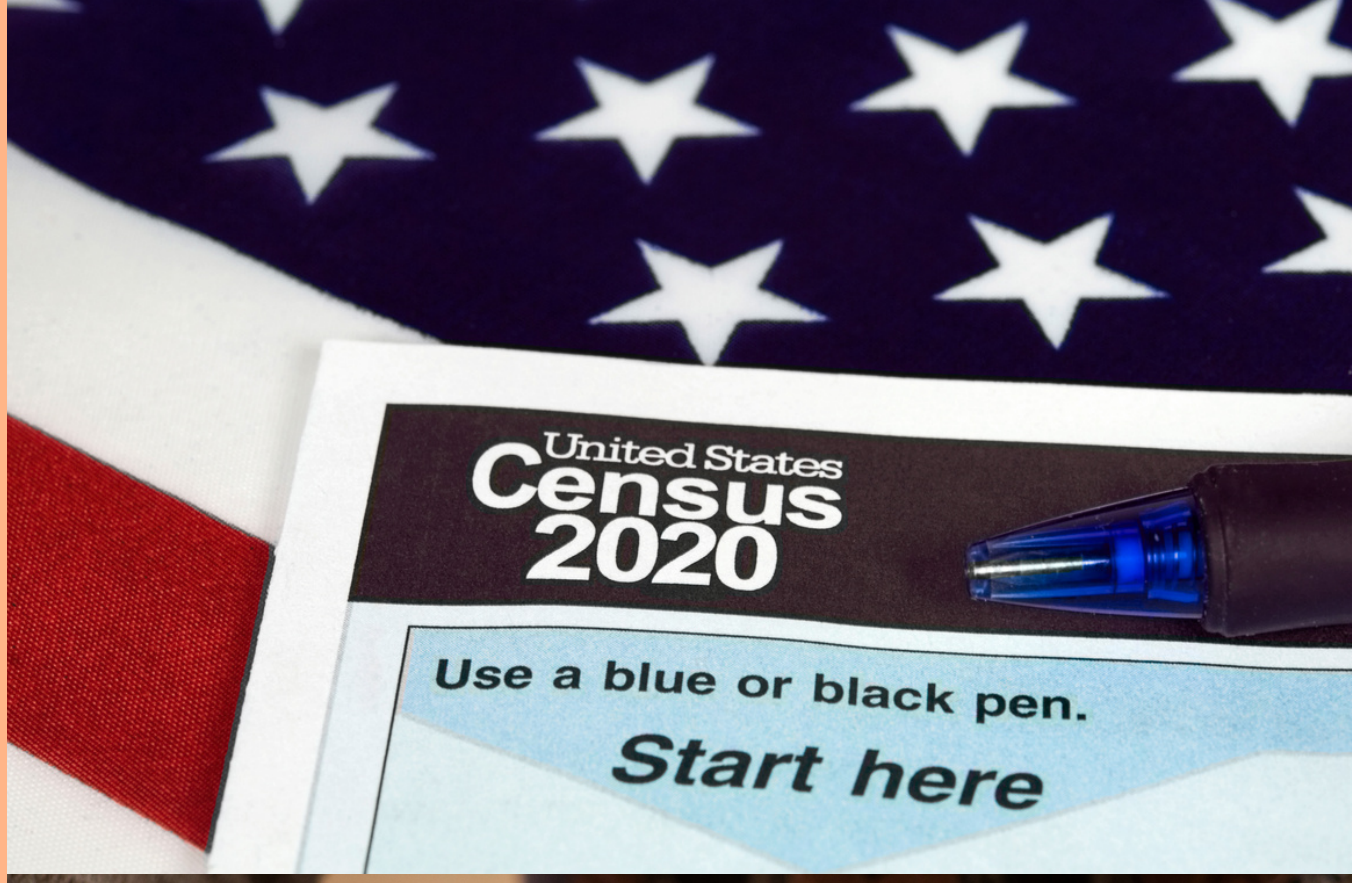
8. Push the FCC to open up more unlicensed and shared spectrum to support Wi-Fi, with a focus on current proceedings on the 5.9 and 6 GHz bands.

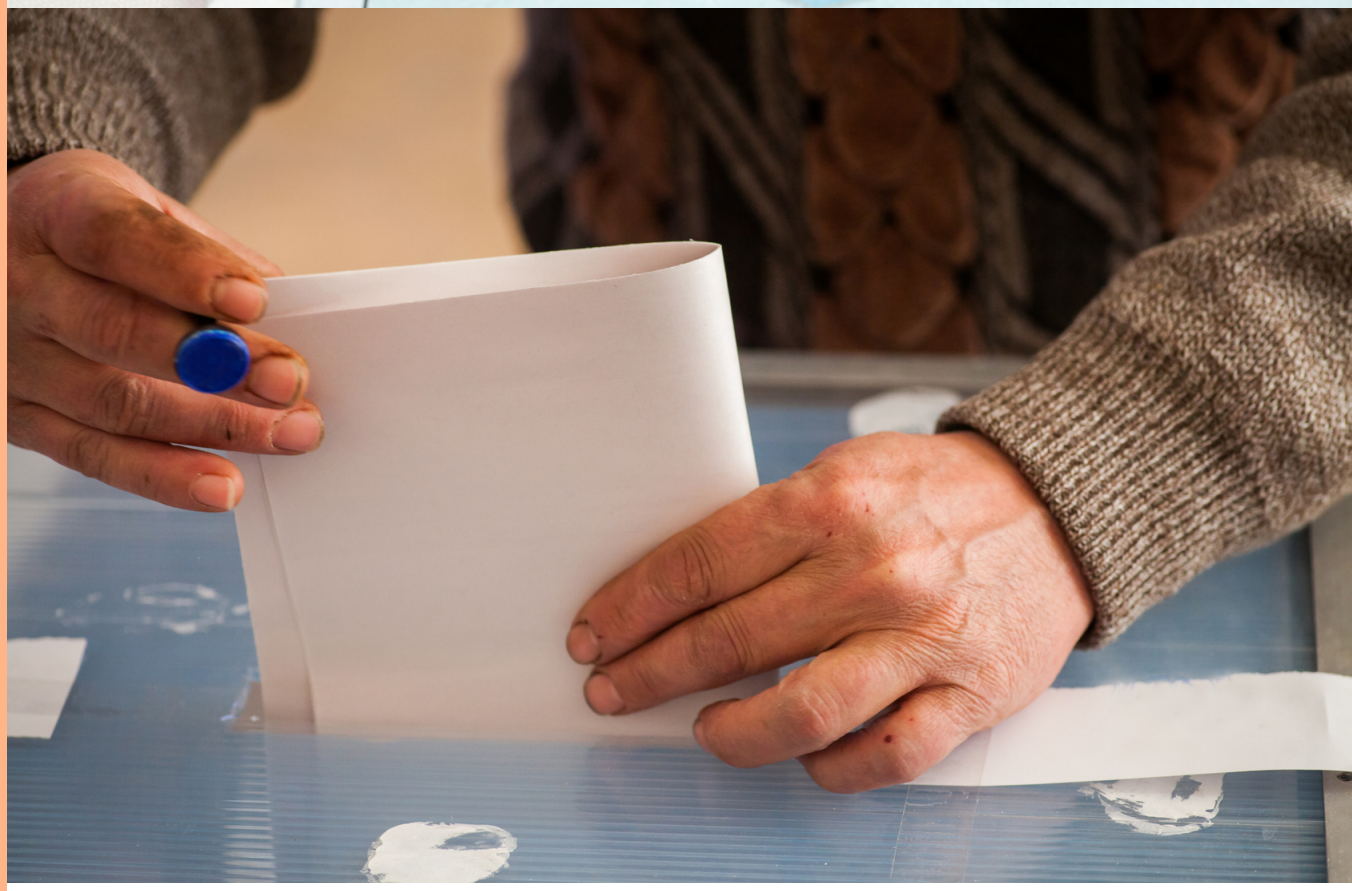
9. Push Internet service providers to open up their hotspots for more open access, particularly during the COVID-19 pandemic.

Digital Redlining

10. Investigate "digital redlining," with a focus on major ISPs' practices of deploying older broadband technologies and slower speeds in low-income areas and communities of color while upgrading technologies elsewhere. This oversight activity should support efforts to pursue additional legislative remedies that require ISPs to provide equal service throughout their service areas as needed.

11. Include questions about efforts to prevent digital redlining in regular FCC oversight hearings.





Democracy: Voting, the Census, and Hateful Content Online

Democracy: Voting, the Census, and Hateful Content Online

Overview

Today, technology is a vital component of our democracy. It helps us stay connected, get informed, and organize for social change. As seen in recent protests against police violence and for racial justice, social media gives communities of color more power to tell their own stories and advocate for change. In effect, online platforms have become the public square for information and discourse.

But, unlike public squares of the past, these platforms enable us to instantaneously reach thousands, or even millions, of people all over the world. This reach creates complex free expression questions requiring greater work to preserve constitutional principles and protect civil rights online. And at the same time, these platforms can be vectors for spreading conspiracies, propaganda, targeted disinformation, and dangerous and discriminatory hateful content often targeted at people of color, religious minorities, women, and transgender and gender-nonconforming people. The January 2021 attack on our Capitol provides a striking example of what can happen when online hate and misinformation proliferate, but it is far from the only one.

The internet plays an increasingly vital role in other parts of our democracy as well. 2020 marked the first time there was a widely available internet response option for the census, creating new challenges for both respondents and the federal government, which had to procure new technological tools. This constitutionally mandated decennial count affects apportionment, congressional redistricting, the distribution of federal resources, and numerous other uses. In recognition of our nation's sharp digital divide (discussed in depth earlier in this document) and the impacts of COVID-19, we must learn the lessons from this decision to ensure a full count in future years.

Tech companies and the federal agencies that oversee them must take their roles in both these opportunities and challenges seriously, in a nonpartisan manner that encourages open participation in voting and the census. Online voter suppression is a serious, persistent threat that requires sustained effort from technology companies to fight it. These companies must improve processes and work on solutions that address the spread of content — from user accounts, ads, organic posts, and groups — that is used to suppress voting and participation in the census by African Americans and other historically marginalized communities.

Similarly, companies should adopt and consistently enforce clear policies that prevent the spread of other targeted disinformation and combat white supremacist and other hateful content on their platforms. These policies should be implemented with a focus on quality rather than quantity, enforced consistently, and come with reasonable due process protections. Important protections include a notice that specifies the reason for content removal, account suspension, or intermediate penalties; a right to appeal any enforcement action; and regular transparency reports detailing a platform's numbers regarding removal, suspension, and any other enforcement actions. The development and enforcement of these protections should involve a diverse set of leaders within the company with relevant expertise and real decision-making authority. Congress must hold companies accountable for doing so, building from the work of multiple committees in the 116th Congress.

Democracy: Voting, the Census, and Hateful Content Online
Recommended Oversight Priorities for the 117th Congress

Online Voter Suppression Policy, Disinformation, and Political Advertising

1. Solicit, and if necessary, subpoena, information from major platform companies including Facebook, Twitter, and YouTube to document their enforcement of community standards policies on voter engagement and civic activities in the 2020 elections and plans for adjustment moving forward. These information demands should include specifics on the implementation of procedures to ensure policies are applied consistently; detailed data on enforcement actions taken, such as removal, labeling, downranking, and other mitigation strategies to address voter suppression (including information on human-driven and automated interventions); and information on volumes and trends. They also should include an inquiry into the applicability of tools deployed to mitigate disinformation on COVID-19 and other issues to addressing voter suppression and false claims of election fraud.

Hateful Online Content

2. Solicit concrete data and additional information from platform companies about key topics related to their removal of hateful content, including:

- Demographic reports and impact assessments that address how content moderation policy affects different communities using the platform, including which communities face the most removals for violating platform rules against hate speech, terrorist content, voter misinformation, harassment, and more.

- Removal procedures, including use of automated tools in the context of every content policy that addresses hateful conduct, the specific types of automated techniques deployed, error rates, and algorithmic biases. This information should also include details on how decisions about whether to use automated tools or human intervention are made.

- Volume of content removals and reasoning for enforcement actions, as well as comparable data for decisions to leave content up after repeated flagging by users and trusted flaggers.

- Volume of appeals, including the number of successful and unsuccessful appeals, information about whether appeals were processed by humans or by an automated system, and the reasoning provided to users to understand a platform's decisions and shape future behavior.

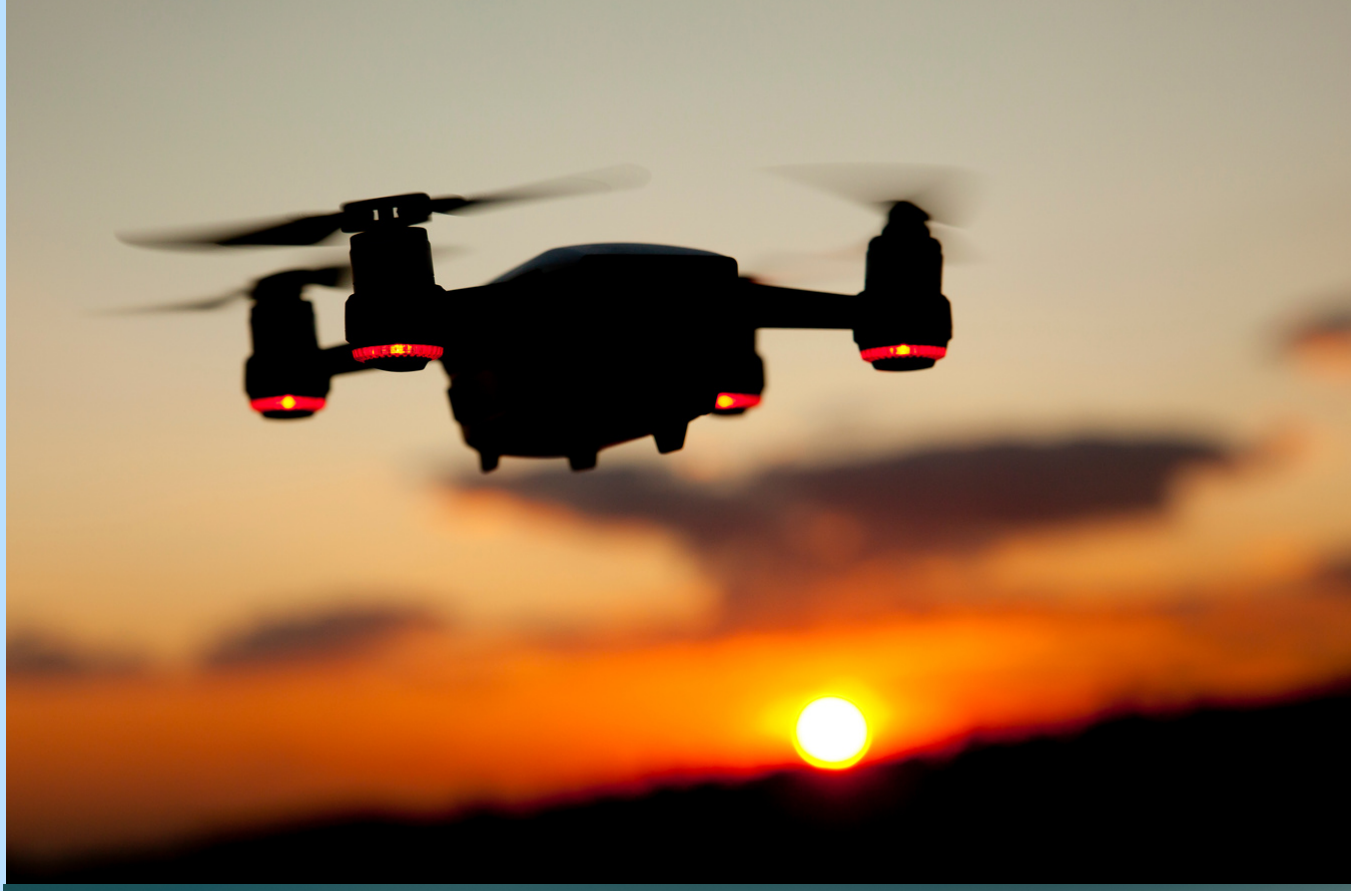
- Use of contractors, permanent employees, and automated tools for content moderation, including cultural training and language capacity.

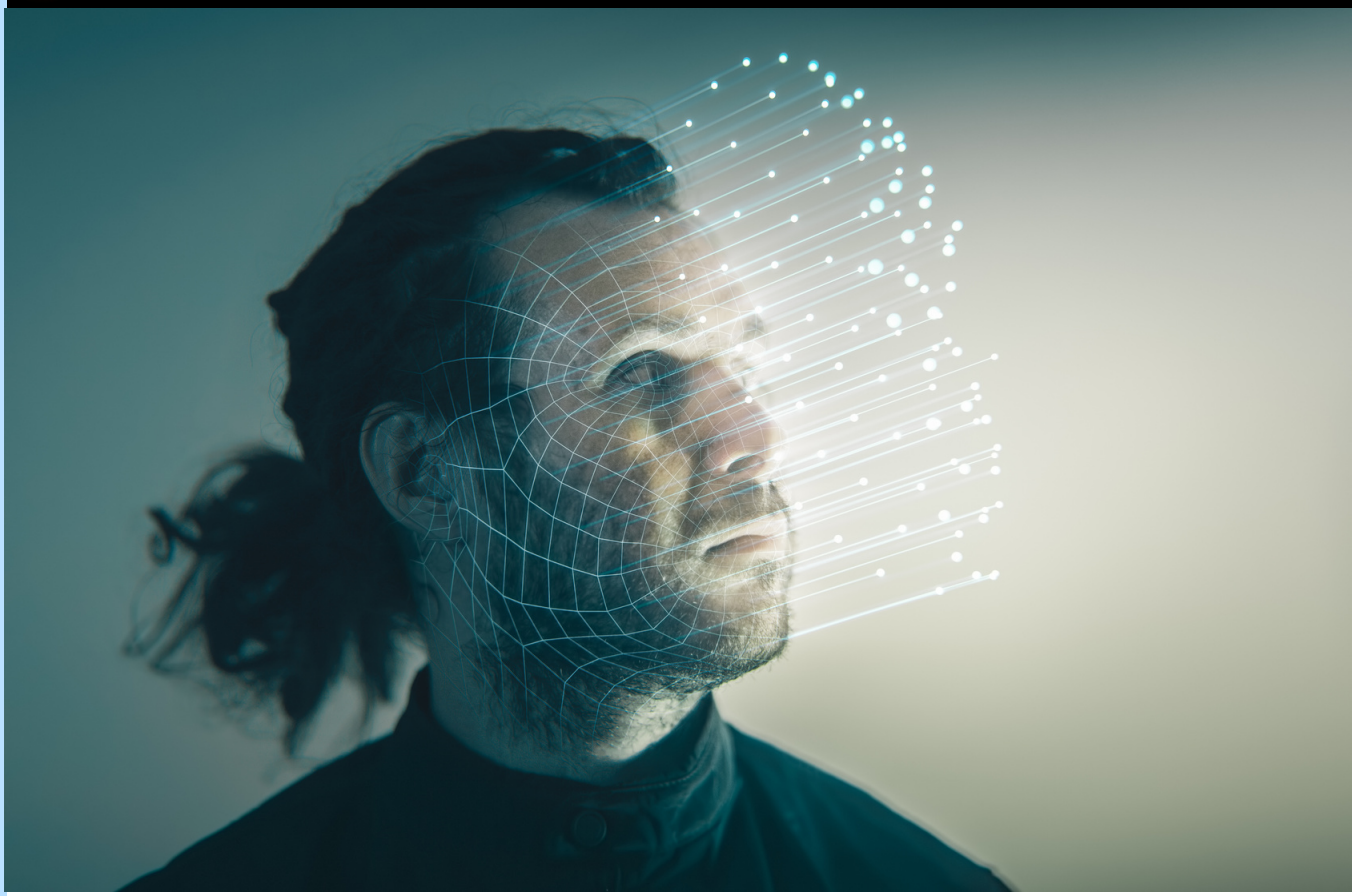
- Mental health support and internal policies that establish protections for content moderators who view violent or disturbing content.

3. Ensure all hearings on Section 230 reform and related topics include perspectives from impacted communities.

Census

4. Conduct an oversight joint hearing with the Census Bureau, FCC, and the Commerce Department on the impacts of an "online-first" census, how the digital divide affected census participation, how the COVID-19 pandemic exacerbated these issues, and the potential impacts on underrepresented communities. This hearing should identify lessons for the 2030 census as well as important research in the intervening years, such as the ACS and the federal data structure in general.





Policing and Justice

Policing and Justice
Overview

The United States is currently undergoing a reckoning of how our country's systems of justice and policing disproportionately harm people of color. Aggressive oversight of policing and justice technology must be a key part of that conversation.

The recent racial justice uprisings across the country have drawn attention to the wide array of surveillance technologies that law enforcement uses, especially to monitor people of color. These tools include everything from social media monitoring and cell site simulators to facial recognition technology, aerial surveillance, and drones. Law enforcement reliance on invasive technology also extends to purchasing access to sensitive data collected by data brokers, **use of aggressive forensic tools on mobile devices**, and wide-ranging demands for location information. Moreover, despite widespread use of these forensic tools to pry sensitive information from devices and data streams, law enforcement entities are demanding privileged access to encrypted communications, which would undermine the security of communications. These tools and privileged access demands have tremendous reach and pose a serious threat to constitutional rights, particularly those guaranteed by the First and Fourth Amendments.

Problematic uses of technology within our policing and justice system do not end at surveillance and investigatory tactics. "Predictive policing" algorithms use massive amounts of historical crime information, and proponents claim these tools can then predict and help prevent potential future crimes by better allocating police resources.

Yet, using **algorithms** to forecast crime **risks** creating a vicious cycle that effectively uses historical data generated by over-policing in areas with large populations of people of color to justify more aggressive policing in those areas moving forward. **Risk assessment algorithms** used in the justice system to inform pretrial decisions, bail, sentencing, and other contexts also pose similar dangers and threaten civil rights protections for equal justice under law. (A **2016 study conducted by ProPublica**, for example, found one common tool systematically assigned Black defendants to a higher risk category than white defendants.) As these tools proliferate in states and localities, as well as within the federal prison system, these risks become even more concerning.

As law enforcement and our government more broadly reckon with the violent assault on the Capitol, it is important that these events are not used to justify expansions of surveillance and other policing policies that disproportionately impact communities of color. Congress must use its oversight powers to decelerate, and where possible stop, the development and deployment of policing and surveillance technologies that impair human, civil, and constitutional rights. In recent years, Congress has sent oversight letters to federal agencies on surveillance issues and held a series of important oversight hearings on facial recognition technology, but that oversight has not included any serious inquiry into the experiences of communities subject to surveillance and over-policing. Future hearings should solicit the expertise of those most impacted by these technologies. Areas of focus should also include surveillance of protests, law enforcement purchases from data broker companies, use of location data and tracking, and forensic investigations of mobile devices.

Policing and Justice
Recommended Oversight Priorities for the 117th Congress

Surveillance of Constitutionally Protected Activity

1. Demand information from federal law enforcement agencies and hold oversight hearings regarding collaboration and data sharing between the federal government agencies and state and local police departments.

- These efforts should pay particular attention to cell site simulators and high-altitude aerial surveillance (both by drones like those **CBP flew over Minneapolis** and manned aircraft like the **Persistent Surveillance program in Baltimore**).

- More broadly, oversight hearings should focus on the use of surveillance tools against protesters and on seeking information as to how this data is used.

- Hearings should also consider such collaboration and data sharing connected to the implementation of the Department of Homeland Security's Targeted Violence and Terrorism Prevention (TVTP) strategy, including with respect to the surveillance, retention, and dissemination of social media data.

2. Investigate particular techniques that were reported in connection with recent protests, including acquisition through unknown means of protesters' **encrypted text messages.**

3. Conduct hearings on the use of social media by the FBI and the Department of Homeland Security to monitor and track activists and protesters, both **historically** and in **recent months.**

- This exploration should include, but not be limited to, use of social media pursuant to President Trump's executive order and **related guidance** on protection of statues and monuments.

Facial Recognition

4. Build from high-impact hearings in the 116th Congress by conducting hearings in multiple committees on facial recognition technology, especially its use by law enforcement. Potential foci could include: impacts of wrongful police actions driven by facial recognition, racially biased policing, and the impacts of facial recognition paired with body-worn cameras.

5. Solicit information from developers of facial recognition tools related to bias and accuracy, including information on training data, diversity of development staff, and auditing/validation procedures.

6. Request the President's Council of Advisors on Science and Technology (PCAST) and the Office of Science and Technology Policy (OSTP) conduct a formal study of the racial bias and due process concerns underlying police use of facial recognition.

7. Request additional GAO reports on facial recognition as needed to collect further information.

Risk Assessment Tools

8. Conduct a series of oversight hearings on risk assessment tools, including ICE's Risk Classification Assessment tool, PATTERN (implemented as a result of the First Step Act), and the Pretrial Risk Assessment (PTRA) for the federal pretrial process. Additional hearings could explore major state and local risk assessment tools. Hearings should seek to explore topics including:

- Algorithm development process, including validation, auditing, and racial impact assessment provisions.
- Impacts and outcomes to date, especially on people of color and including granular data on use of these tools to inform decisions on release, conditional release, house arrest, electronic monitoring, and mandated programs.
- Use of risk assessments in decarceration efforts, including, but not limited to, those undertaken in response to COVID-19.
- Changes in scoring procedures.
- School behavioral threat assessments that are aimed at preventing violence in schools.

9. Request similar information from manufacturers of major risk assessment tools used by states and localities, including Equivant (formerly Northpointe). This information request should be used to explore development, validation, auditing, and racial impact assessment procedures.

10. Commission a GAO report on the use of risk assessment instruments in federal and state justice systems with a focus on decarceration. Such a study should collect information on:

- Racial impacts, including practices/processes to ensure racially equitable decarceration.
- How risks assessments are used (including under what circumstances, by which agencies, and whether they are used independently or in conjunction with other pre-trial systems).
- What impacts these tools have on release of incarcerated individuals, including specific data on range and incidence of release and conditions as well as analysis of changes in release conditions and outright release.
- The data from which risk assessments are developed and validated, as well as procedures and frequency for ongoing validation or reassessment efforts.
- Decision-making frameworks associated with the risk assessment instruments.

11. Conduct an oversight hearing examining any technological risk assessment tools being developed or used in support of the Department of Homeland Security's goal of "identify[ing] and respond[ing] to individuals at risk of mobilizing to violence" as part of its broader Targeted Violence and Terrorism Prevention (TVTP) strategy.

Reverse Location Searches

12. Conduct a hearing with law enforcement agencies, technology companies, and public interest organizations to explore civil rights implications of the growing use of reverse location searches, including "geofence warrants" and tower dumps, which obtain information about all mobile devices in an area at the time of a suspected crime.

13. Solicit information from federal law enforcement agencies and technology companies about the use of reverse location searches, including frequency of requests, the legal process followed, the service providers that provide this location data, total number of requests and affected users, procedures for data minimization, outcomes of requests, and other information needed to support policy reform.

Law Enforcement Purchase of Location Data and Partnerships with Data Brokers and Other Stakeholders

14. Conduct oversight hearings to examine law enforcement and intelligence use of private industry, particularly data brokers, to obtain sensitive information about the public, such as location data. Oversight letters and subpoenas could be used to gather additional information from relevant data broker companies if needed. This information request should build on existing efforts to investigate Venntel and other companies that sell location data in any form.

15. Direct the GAO to study federal and state use of private databases and contracting with private companies for law enforcement or surveillance purposes, including, but not limited to, Ring, Clearview AI, Sensorvault, and Venntel.

16. Conduct oversight hearings to examine the intersection between public health surveillance and surveillance for criminal or civil enforcement. Critical topics for discussion include:

- The nature and scope of data sharing between public health officials, researchers, or experts on the one hand and law enforcement or immigration agencies on the other.
- The consequences of such sharing.
- Policy options to remedy identified problems.

Predictive Policing

17. Conduct oversight hearing series on predictive policing tools, focusing on civil rights, racial justice, and equity questions, as well as efficacy.

18. Solicit information from manufacturers of predictive policing tools such as PredPol, inquiring about data related to racial impacts, reliance on historical data, approaches to adjusting for past bias in policing, measurements of impact/effectiveness, auditing for disparate impacts, and other topics important to protecting civil rights.

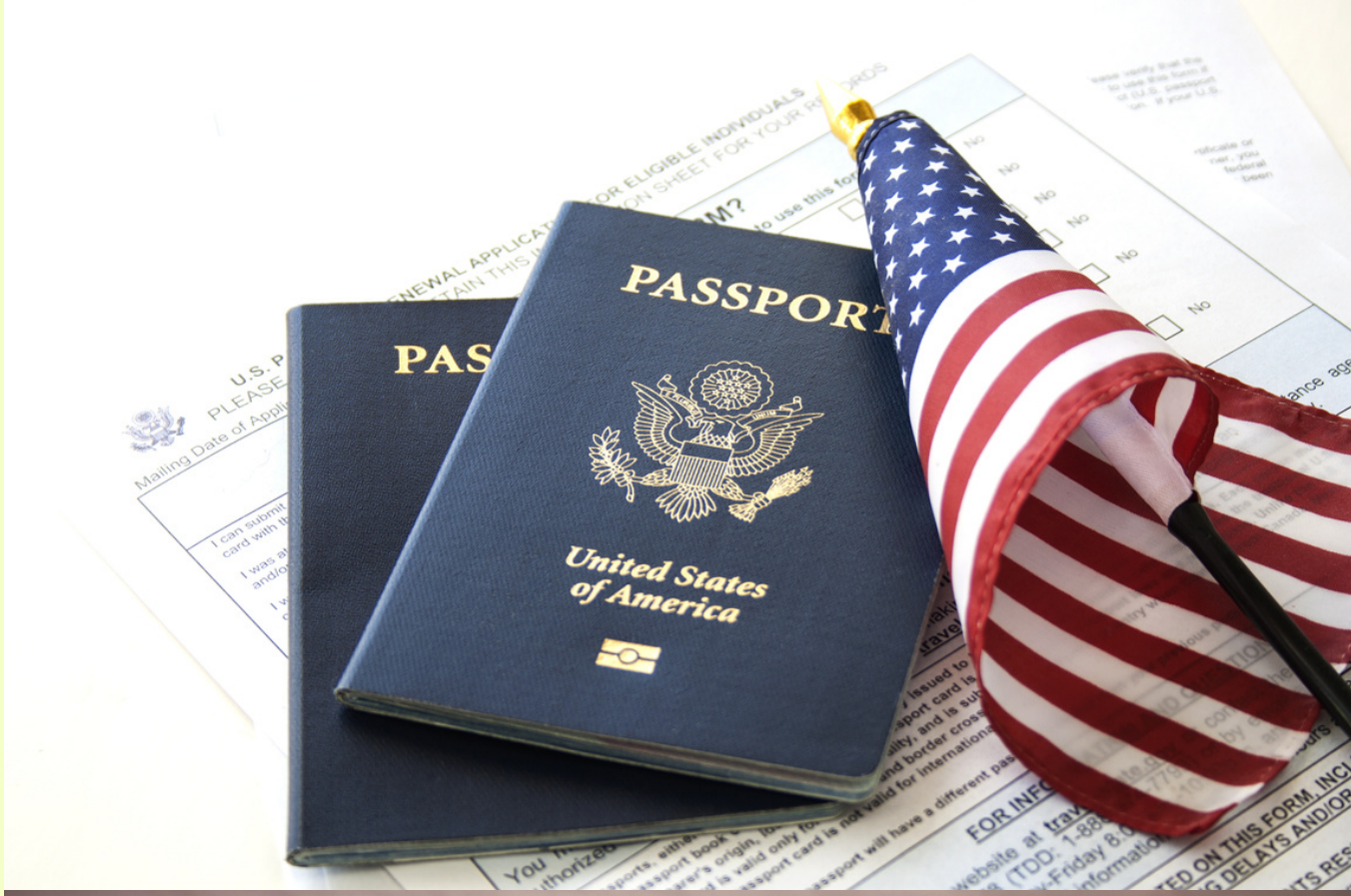
Mobile Device Forensic Tools

19. Request information from relevant federal agencies about the tools they use to extract and analyze information from devices. This information gathering should include exploring the use of federal Regional Computer Forensics Labs, including what technology they use, how it has been validated, what kinds of cases it is being used in, and procedures related to local law enforcement uses of the labs.

20. Conduct hearings on the extent to which federal agencies are accessing data in an unencrypted form that is in transit, stored on personal devices, or stored by communications service providers.

- Request a full accounting of the number of demands for compelled disclosure of stored communications content federal government agencies made over a one-year period, and a full accounting of the number of such demands that could not be complied with because of encryption.

21. Request the GAO produce a study of these issues.



Immigration Surveillance Technology

Immigration Surveillance Technology

Overview

America is a nation founded and built by refugees, immigrants, and those seeking religious freedom. Yet in recent years, the federal government has waged a deeply troubling and persistent campaign against immigrants arriving to and living in our country. Instead of welcoming those seeking opportunity or fleeing persecution, our government has stripped immigrants of their status, reduced due process protections, targeted people for harassment, and torn families apart. The implementation of automated systems and technologies to surveil individuals and make decisions in our immigration system has only further threatened immigrants' rights and represents another troubling pattern of dehumanizing these individuals.

The problematic uses of surveillance and other invasive technologies to target immigrants and abet these abuses are myriad. Despite evidence that the collection of social media data for national security vetting and immigration enforcement purposes is ineffective, discriminatory, and stifles free expression, the Department of Homeland Security and the Department of State have expanded privacy-invasive programs to collect and monitor visitors' and immigrants' social media handles and communications. DHS increasingly turns to technological tools — often leveraging off-the-shelf systems procured from private vendor companies — to automate and systematize DHS's surveillance of immigrants at the border and across the United States. The use of these tools has dangerous, chilling effects on free speech, free expression, and association.

Unfortunately, Congress has permitted these tools to grow unchecked, largely ignoring the dangers of allowing the Department of Homeland Security to tap into this wealth of information for immigration decisions. There have been some limited exceptions — most notably the Congressional Black Caucus's powerful call that helped prompt ICE to back away from its discriminatory Extreme Vetting Initiative, which would have used an automated social media scan to flag "threats" and wrongly target immigrants of color and specific religious groups. Moving forward, Congress must substantially increase its oversight on these matters, while also taking on the government's expanding contracts with surveillance vendors.

Immigration Surveillance Technology
Recommended Oversight Priorities for the 117th Congress

Social Media Monitoring

1. Investigate the Department of Homeland Security and the Department of State's invasive and unnecessary programs to collect and monitor social media handles and communications of visitors and immigrants, including U.S. persons. This effort should engage civil society and should focus particularly on the impact of these programs on Muslims and other historically targeted groups; it should also explore the legality of these programs and the likelihood that they are overbroad, ineffective, and discriminatory, while stifling free speech. This oversight effort must include an examination of federal policies and practices applicable to the social media screening of immigrants and travelers and the extent to which those policies and practices are documented and sufficiently thorough, appropriately account for civil rights and liberties concerns, and permit accountability for abuses.

2. Hold hearings with industry professionals and relevant government agencies to gain an understanding of the current scope of social media monitoring technology capabilities and their limitations.

3. Request that GAO conduct a review of DHS's and the State Department's collection and use of social media identifiers in connection with the screening of travelers and individuals applying for immigration-related benefits.

Immigration Surveillance Technology

4. Conduct an oversight hearing on DHS's use of invasive surveillance technologies targeting immigrants at the border and in the United States, as well as surveillance of lawyers, journalists, and advocates at the border.

5. Conduct an oversight hearing on how DHS and DOJ classify and monitor the activities of groups they categorize as "gangs," including through the maintenance of the Transnational Criminal Organization watchlist. This hearing should examine how this watchlist impacts rights to due process, equal protection, and free association.

6. Request a new or updated GAO study of DHS's (including ICE and CBP's) contracting for and purchase of surveillance technology and automated decision-making tools, including those provided by Palantir and other major vendors. To the maximum extent feasible, this study should include an exploration of the use of "off-the-shelf" tools.

7. Collect information and conduct a hearing if needed on CBP's use and expansion of biometric data on entry/exit at airports, ports, and borders.

8. Work with state and local stakeholders to secure executive actions to cut off or dramatically reduce flows of sensitive data from state and local governments and the private sector to ICE.

Commercial Data Practices and Privacy

Commercial Data Practices and Privacy

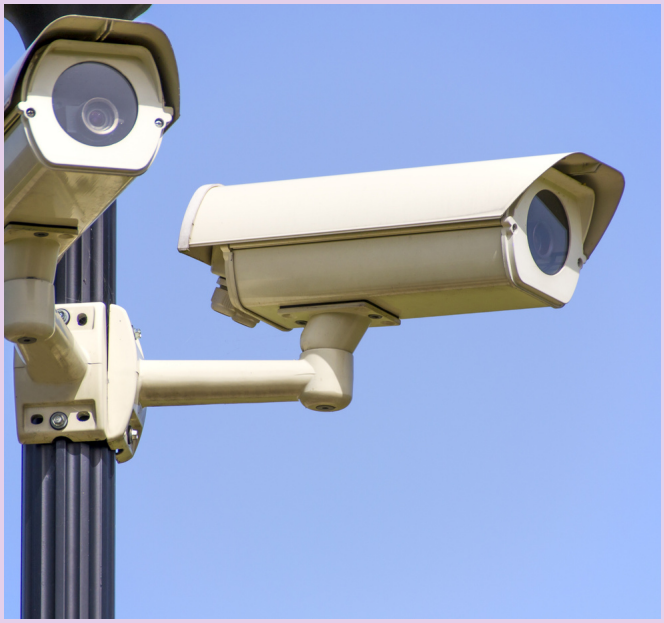
Overview

It is essential: the United States needs comprehensive national privacy law. The lack of regulation of commercial data practices leaves everyone vulnerable to abusive practices, but historically marginalized communities and communities of color are even more at risk. Today, the primary protections most adults have are inadequate select state and sectoral privacy laws. Most of these extant privacy laws do not contain anti-discrimination protections or effective enforcement provisions, such as a private right of action.

Unchecked data collection and minimal regulation of its use can exacerbate inequities in our society. Profiles and scores compiled by data broker companies can be used to exclude people from opportunities or target them for predatory services. Growing private use of facial recognition technology can be used to ban people from stores or target them for additional assistance without their consent or knowledge. As seen through the massive data breaches that have occurred in recent years, large-scale data collection can put information at risk of theft, and this data could be used for unrelated purposes, like employee monitoring or law enforcement. And the shadowy market for location data can expose sensitive information to stalkers, marketers, and others.

These are just a few of the many harms a comprehensive privacy law and more aggressive regulation could help prevent. However, existing authorities should be used to protect the public as well, and Congress must act to ensure existing authorities are deployed while efforts to build more comprehensive and thorough protection are underway.

Congress has a vital role to play in deterring bad behavior by private actors and in ensuring federal regulators are taking these threats seriously. In some cases, the Federal Trade Commission has taken important action to crack down, using its powers to counter unfair or deceptive practices; in others, its enforcement actions have effectively normalized data violation fines as a cost of doing business, rather than a real deterrent. Congress must demand more aggressive action from regulators tasked with monitoring these behaviors and preventing abuses.



Commercial Data Practices and Privacy
Recommended Oversight Priorities for the 117th Congress

Data Privacy

1. Conduct robust, ongoing oversight of the Federal Trade Commission to ensure it:

- Investigates, challenges, and punishes abusive commercial data practices, especially with respect to existing consent orders with major technology companies.
- Invests adequately in expertise on equity and civil rights issues, as well as internal technical capacity, to oversee technology companies.
- Issues guidance and brings enforcement actions that apply the Unfairness Doctrine to discriminatory practices using a broader understanding of harm.
- Engages in Magnuson-Moss rulemaking to address commercial data practices.
- Enforces violations of the Children's Online Privacy Protection Act.

2. Conduct an oversight hearing to hold federal agencies accountable for prioritizing enforcement of existing civil rights laws on online platforms, including in housing and employment. This hearing should include representatives from the DOJ Civil Rights Division, Department of Housing and Urban Development, Department of Labor, and other agencies as appropriate.

3. Demand relevant executive branch agencies report on how personal data is used within their areas of jurisdiction, whether such data can be or is being used discriminatorily, and whether regulations to address such discrimination are necessary (using existing authorities or seeking new ones).

4. Conduct oversight hearings to hold federal, state, and local practitioners, as well as the companies that work with them, accountable for protecting the privacy rights of students. Hearings should address the impact of COVID-19 on education data, technology, and student privacy and represent the perspectives of those who are responsible for student privacy, state and local education agencies, as well as those who are most affected, students and their families.

5. Hold oversight hearings on privacy harms, algorithmic accountability, and historically marginalized communities to explore the ways in which today's inadequate protections can uniquely harm people of color and other marginalized communities. Preparation for these hearings should include demanding (with subpoenas, if necessary) material from relevant companies with respect to the targeting of predatory advertising and algorithmic accountability, including their procedures for ensuring compliance with civil rights laws.

Public Health Technologies

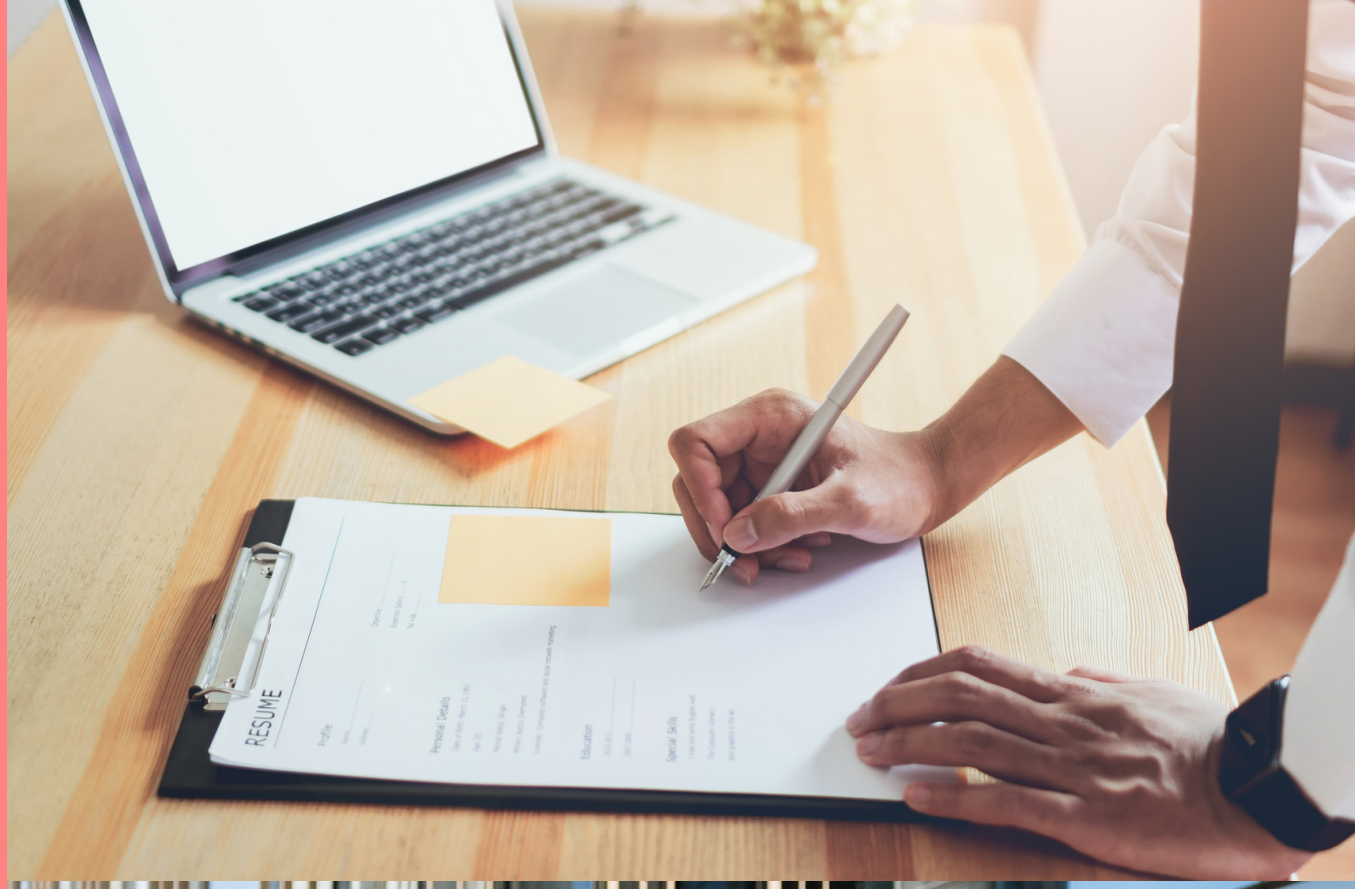
6. Hold hearings to examine the collection, use, and dissemination of data connected to public health efforts, including location data (even if it is de-identified and/or aggregated), whether by governments, researchers, nonprofit organizations, or private firms. Congress may examine:

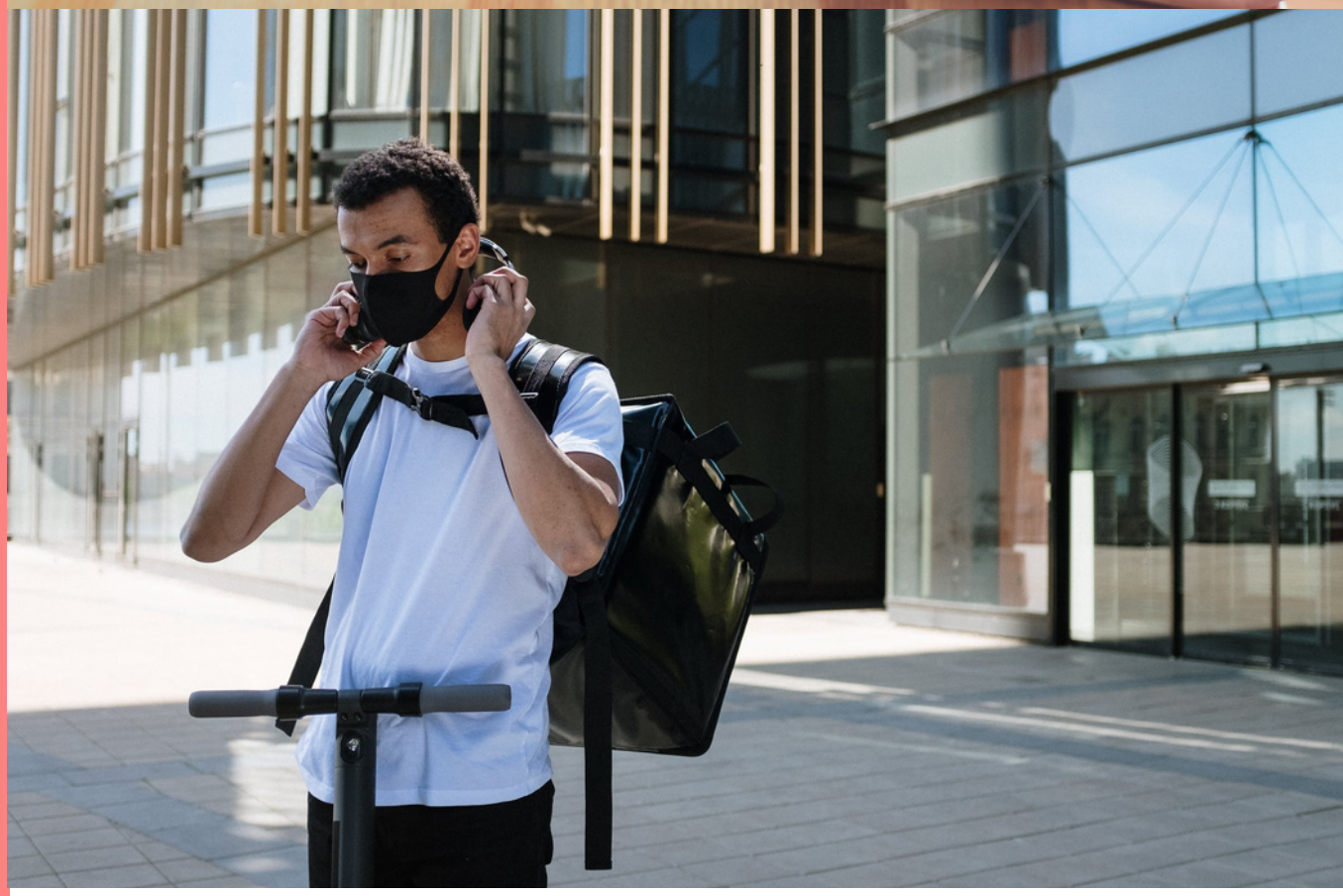
- The efficacy of mobility data to achieve the public health purposes for which it is used, especially given the involvement of unspecialized corporate actors in many of these efforts, and the absence of uniform data quality and methodological standards.

- The tailoring of data use and granularity to public health needs.

- The landscape of data privacy rules and practices relevant to the collection, use, and dissemination of data in the public health context, and the impacts of identified regulatory gaps, including on public trust in disease containment initiatives. Such an inquiry may involve requesting information about in-house data security and privacy protections from developers of major COVID-19 contact tracing apps, from data broker firms sharing or selling data to inform public health decisions and research, or from other relevant institutions, such as universities or state and local governments. It may also involve examining laws applicable to the privacy or confidentiality of such data (for example, the Stored Communications Act, HIPAA, and HITECH).

- The sharing of information between public health experts/officials and law enforcement and immigration agencies, and the consequences of such sharing.





Workers, Labor, and Hiring

Workers, Labor, and Hiring

Overview

Workers in the United States have few meaningful protections against surveillance under current law. While data dictates many of the decisions in today's workplace — like hiring, firing, promotion, and discipline — workers are largely in the dark about what data is collected, how it is obtained, and how it is used. As more employers deploy tools to avoid the spread of COVID-19 and trace contacts, these questions are more relevant than ever.

Opaque hiring assessment technologies that use algorithms and other techniques to select job candidates mean today's workers even face the threat of discrimination before they are hired. Building from historical hiring data, these tools can reinforce patterns of discrimination and/or ensure underrepresented communities might not even have a chance at an interview.

Workplace surveillance and hiring assessment technologies alike support discrimination and exacerbate the power and information asymmetries in the workplace that often put people of color, women, and those with disabilities at the bottom. Early in 2020, in recognition of these challenges, leading civil rights, research, and advocacy organizations **issued principles** for the equitable development, use, auditing, and oversight of hiring assessment technologies.

Our country has a mixed, but vital history of creating legislation to protect workers' rights and enforce nondiscrimination in the workplace, including prohibitions on harmful actions based on sex, race, national origin, religion, age, and disability. Recognizing changes in technology, those protections must be modernized, strengthened, and expanded to better apply civil rights protections to workers' data and technological tools in the hiring process. Public interest organizations have created a variety of **reform proposals** that Congress should explore.

Nonetheless, existing protections are far-reaching and should be enforced where they can to mitigate or eliminate harmful practices while further reforms are pursued. Congressional oversight is vital to ensure that government agencies enforce existing protections vigorously and companies do not use technical tools to hide discrimination (or even expand its scale by automating decision-making). The priorities identified here are designed to ensure the federal government is leading on these issues appropriately, as well as build an evidence base to better inform effective policymaking.

Workers, Labor, and Hiring
Recommended Oversight Priorities for the 117th Congress

Hiring Assessments

1. Conduct a hearing with relevant Equal Employment Opportunity Commission leadership to ensure the agency appropriately prioritizes enforcement of existing nondiscrimination provisions with respect to hiring assessment technologies.

2. Hold a hearing with providers of major hiring assessment technologies and public interest organizations to explore how these technologies comply with existing nondiscrimination law and where additional reforms are required. Congress should request or subpoena if necessary relevant technical documentation to assess validity of these claims.

3. Review the work of the Office of Federal Contract Compliance Programs in conducting compliance evaluations and investigations of federal contractors' and subcontractors' personnel policies and procedures to enforce nondiscrimination provisions with respect to hiring assessment technologies and AI.

4. Direct the GAO to study:

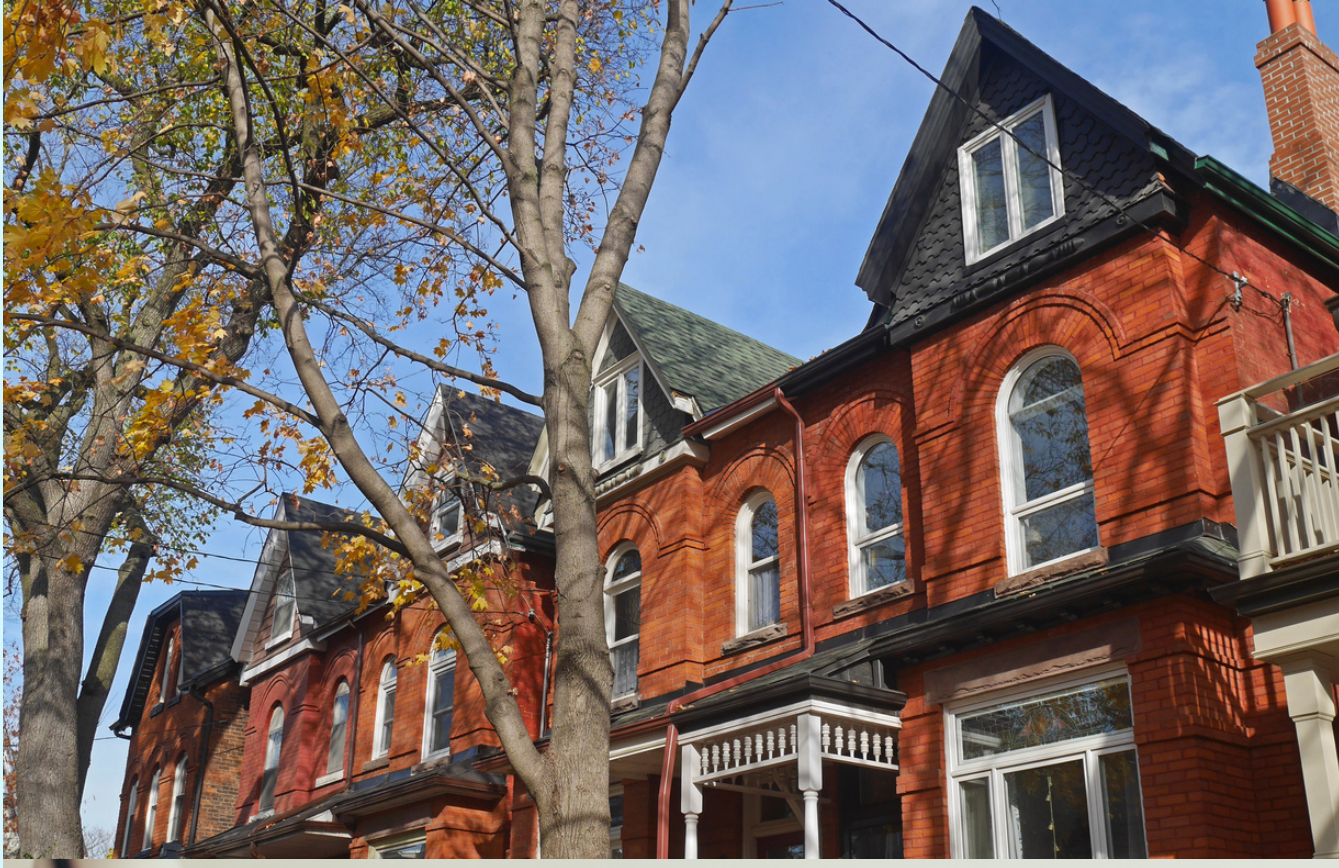
- Federal and state government use of hiring assessment technologies.
- Federal contractor use of hiring assessment technologies.
- Federal government use of behavioral data collection on employees, decision-making involving such data, and related issues.

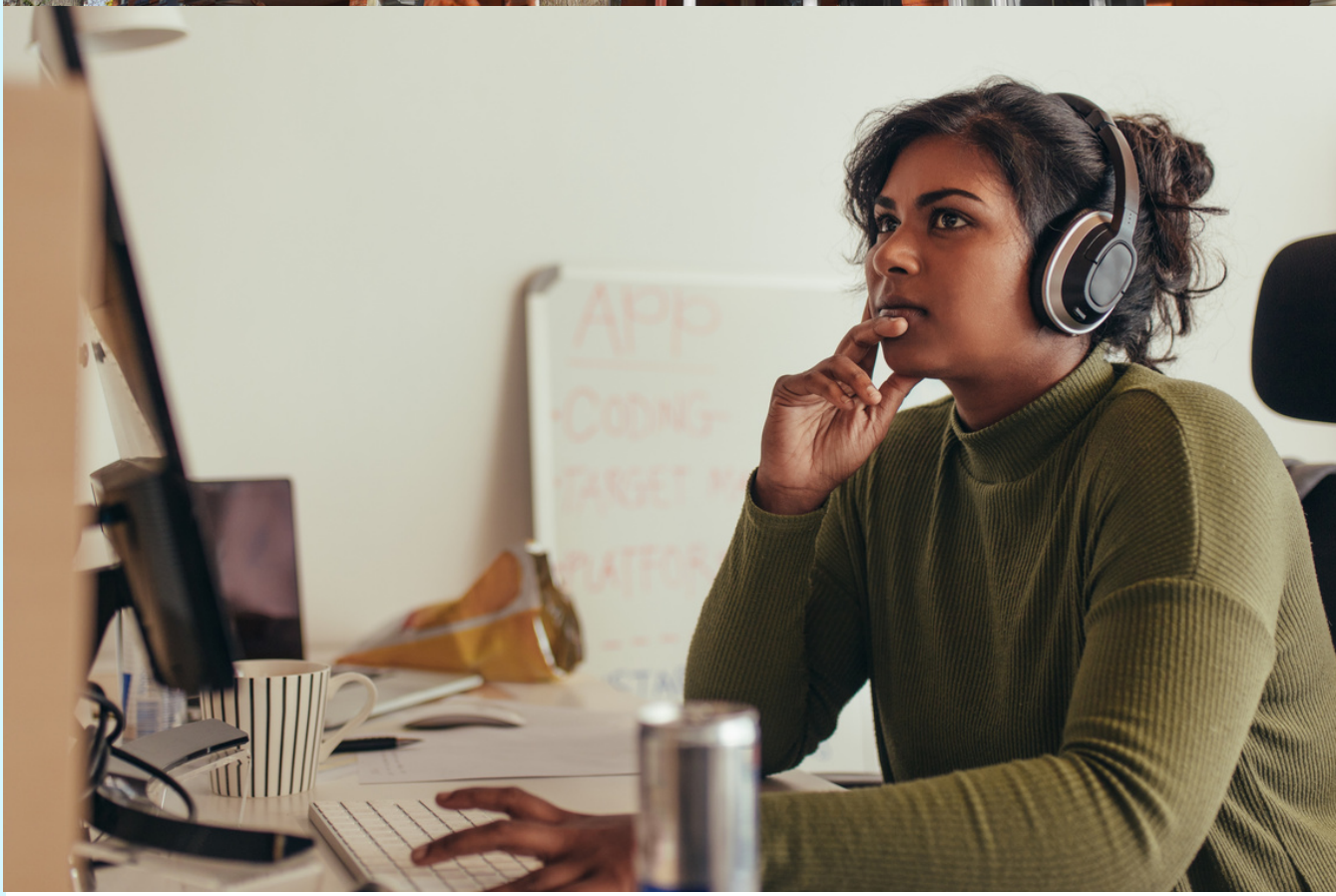
Worker Surveillance and Privacy

5. Conduct a hearing with relevant Department of Labor leadership to document how it is protecting worker privacy and data using existing legal authorities, including those under Title VII of the Civil Rights Act. This hearing should also include oversight of **algorithmic scheduling and management issues**.

6. Solicit information from major employers about how their use of technology to mitigate the spread of COVID-19 respects privacy rights of employees, including the collection of biometric information and contact tracing. This initial information request could be followed by a hearing or series of hearings. As appropriate, oversight activities here should include an assessment of compliance with HIPAA and explore the EEOC's efforts to protect worker biometric data.

7. Investigate major employers' use of workplace tracking technologies, like "Time Off Task" to retaliate against workers, undermine safety protections, and/or impede legally protected rights to organize.





Additional Priorities

Additional Priorities

Recommended Oversight Priorities for the 117th Congress

The priorities articulated in this agenda are wide-ranging but not intended to be a comprehensive list of issues on which the 117th Congress should conduct oversight activity. There are many other places Congress's oversight powers should be deployed to address challenges and opportunities at the intersection of civil rights and technology. Below are a variety of additional places Congress can act.

Oversight Capacity

1. Congress should:

- Protect Inspectors General from efforts to undermine their independence, and it should ensure they have the resources and technical expertise necessary to conduct work on issues identified in this report.

- Invest in its own technical staff expertise needed to perform oversight work on these issues effectively.

- Prioritize in its oversight activities efforts to ensure agencies are building and maintaining the in-house technical, civil rights, and equity expertise necessary to protect civil rights in the digital age.

- Support the independence of immigration judges.

Competition

2. Appropriate committees should continue antitrust and economic policy work designed to promote competition in digital services and mitigate the impacts of corporate consolidation. This work should include explicit efforts to analyze and mitigate:

- Negative impacts on businesses owned by people of color.

- Harmful impacts of data monopolies with respect to civil rights law and predatory targeting of underrepresented communities.

- Proliferation of hateful content and dis- and misinformation, especially with relevance to voter suppression efforts.

Representation and Diversity in Tech

3. Major technology companies continue to have extreme underrepresentation of people of color and women in leadership and engineering roles. This fact is concerning in light of the ways in which algorithms developed by these companies harm underrepresented communities and how surveillance tools are used to unfairly track them. Congress should include in its oversight activities efforts to ensure compliance with equal opportunity law and support an inclusive workforce in this key industry. In addition, oversight activity of major technology companies should encourage them to build or sustain civil rights infrastructure within their companies, integrating civil rights expertise at the very highest levels of decision-making.

Additional Priorities
Recommended Oversight Priorities for the 117th Congress

Disparate Impact

4. Congress should conduct oversight to ensure relevant agencies seek to protect disparate impact standards and apply them appropriately with respect to automated decision-making systems. Requests for information or hearings should explore agency efforts to undermine these rules, such as HUD's recent final rule that **makes it easier for landlords to discriminate** in housing if they purchase algorithmic screening tools. This oversight should encourage the modification or withdrawal of these rules that facilitate the use of technology to undermine protections long-afforded in cases of disparate impact.

Algorithmic Accountability

5. To the extent that work outlined in this agenda does not already address bias in artificial intelligence and automated decision-making systems, oversight activity should prioritize investigating the use of these technologies, auditing procedures to detect bias and other risks, compliance with existing laws, impacts on underrepresented communities, and needed policy reforms. Federal agencies should lead on these efforts, and oversight activities should hold them accountable for doing so. Potential targets for this action could include the:

- Consumer Financial Protection Bureau with respect to the use of AI in banking, insurance, and fintech products.
- The Department of Education with respect to student lotteries, testing accommodations, and admissions practices.
- The Department of Justice with respect to DNA-matching algorithms.

6. Oversight activities should also hold federal agencies accountable for their own **increasing use of AI**, which may raise new and important questions about due process, transparency, and accountability in agency decision-making.

7. Additionally, relevant committees (individually or acting in concert) should collect relevant documents and technical materials from major technology companies explaining how their algorithms work, partner with academic researchers, and investigate disparate impacts from algorithmic biases.

Conclusion

It is clear that the United States needs new, updated, and comprehensive laws to protect our civil rights. Technological progress should promote equity and justice as it enhances safety, economic opportunity, and convenience for everyone. Today, racial discrimination in policing, misinformation and disinformation online, lack of home broadband internet, and the economic and health ramifications of the COVID-19 crisis disproportionately affect underrepresented and historically marginalized communities. Especially while updated rules are developed and implemented, Congress must use its existing authorities and oversight powers to protect civil rights.

The current COVID-19 crisis, efforts to promote an economic recovery, and the attack on the Capitol also highlight the urgency of real oversight work. The pandemic has pushed our society out of public spaces and into our own homes and online. Education, health and medicine, work, and civic engagement are occurring online. As millions of unemployed people attempt to return to work, the consequences of algorithmic bias in hiring may be more significant than ever before. The consequences of hate, white supremacy, and misinformation spread through online platforms are far-reaching and terrible.

In this context, Congress must take its oversight responsibilities with technology and civil rights seriously, deploying them as it also pursues relevant legislation as needed. Technology has created tremendous opportunities, and at its best can support a stronger, more-inclusive economy, society, and public sphere. But these outcomes do not occur by chance. Policymakers must work to ensure that technology is designed and used in ways that respect civil rights, preserve privacy, ensure transparency, and hold both nation-states and companies accountable for harm.

This document provides a clear oversight agenda for the 117th Congress to do that critical work of promoting just technology, defending civil rights, and countering abuses. This Congress confronts a pivotal opportunity and a time for leadership. We hope national leaders take these challenges seriously and rise to meet them.

Appendix: Oversight Priorities Sorted by Targeted Organization

This appendix presents the previously recommended priorities sorted by the names of agency or organization these recommendations target for oversight. It is meant to act as an additional resource for those focused on oversight of specific agencies or companies.

Private Companies

Broadband Internet – Disaster Recovery

- Demand information from the FCC and major ISPs about their disaster response and network interruption procedures with a focus on recent disasters such as Hurricane Maria in Puerto Rico and the California wildfires. This demand for information should include additional data collection about network status during and after disasters by ensuring the FCC requires ISPs submit this data.

- Hold a hearing about telecommunications disruptions in the wake of natural disasters, including both major ISPs and organizations representing impacted communities.

Broadband Internet – Wi-Fi and Unlicensed Spectrum

- Push Internet service providers to open up their hotspots for more open access, particularly during the COVID-19 pandemic.

Broadband Internet – Digital Redlining

- Investigate "digital redlining," with a focus on major ISPs' practices of deploying older broadband technologies and slower speeds in low-income areas and communities of color while upgrading technologies elsewhere. This oversight activity should support efforts to pursue additional legislative remedies that require ISPs to provide equal service throughout their service areas as needed.

Democracy, Voting, the Census, and Hateful Content Online – Online Voter Suppression Policy, Disinformation, and Political Advertising

- Solicit, and if necessary, subpoena, information from major platform companies including Facebook, Twitter, and YouTube to document their enforcement of community standards policies on voter engagement and civic activities in the 2020 elections and plans for adjustment moving forward. These information demands should include specifics on the implementation of procedures to ensure policies are applied consistently; detailed data on enforcement actions taken, such as removal, labeling, downranking, and other mitigation strategies to address voter suppression (including information on human-driven and automated interventions); and information on volumes and trends. They also should include an inquiry into the applicability of tools deployed to mitigate disinformation on COVID-19 and other issues to addressing voter suppression and false claims of election fraud.

Democracy, Voting, and the Census – Hateful Online Content

- Solicit concrete data and additional information from platform companies about key topics related to their removal of hateful content, including:
  - Demographic reports and impact assessments that address how content moderation policy affects different communities using the platform, including which communities face the most removals for violating platform rules against hate speech, terrorist content, voter misinformation, harassment, and more.
  - Removal procedures, including use of automated tools in the context of every content policy that addresses hateful conduct, the specific types of automated techniques deployed, error rates, and algorithmic biases. This information should also include details on how decisions about whether to use automated tools or human intervention are made.
  - Volume of content removals and reasoning for enforcement actions, as well as comparable data for decisions to leave content up after repeated flagging by users and trusted flaggers.
  - Volume of appeals, including the number of successful and unsuccessful appeals, information about whether appeals were processed by humans or by an automated system, and the reasoning provided to users to understand a platform's decisions and shape future behavior.

- Use of contractors, permanent employees, and automated tools for content moderation, including cultural training and language capacity.
- Mental health support and internal policies that establish protections for content moderators who view violent or disturbing content.

Policing and Justice – Facial Recognition

- Solicit information from developers of facial recognition tools related to bias and accuracy, including information on training data, diversity of development staff, and auditing/validation procedures.

Policing and Justice – Risk Assessment Tools

- Request similar information from manufacturers of major risk assessment tools used by states and localities, including Equivant (formerly Northpointe). This information request should be used to explore development, validation, auditing, and racial impact assessment procedures.

Policing and Justice – Reverse Location Searches

- Conduct a hearing with law enforcement agencies, technology companies, and public interest organizations to explore civil rights implications of the growing use of reverse location searches, including "geofence warrants" and tower dumps, which obtain information about all mobile devices in an area at the time of a suspected crime.

- Solicit information from federal law enforcement agencies and technology companies about the use of reverse location searches, including frequency of requests, the legal process followed, the service providers that provide this location data, total number of requests and affected users, procedures for data minimization, outcomes of requests, and other information needed to support policy reform.

Commercial Data Practices and Privacy – Public Health Technologies

- Hold hearings to examine the collection, use, and dissemination of data connected to public health efforts, including location data (even if it is de-identified and/or aggregated), whether by governments, researchers, nonprofit organizations, or private firms. Congress may examine:
  - The efficacy of mobility data to achieve the public health purposes for which it is used, especially given the involvement of unspecialized corporate actors in many of these efforts, and the absence of uniform data quality and methodological standards.
  - The tailoring of data use and granularity to public health needs.
  - The landscape of data privacy rules and practices relevant to the collection, use, and dissemination of data in the public health context, and the impacts of identified regulatory gaps, including on public trust in disease containment initiatives. Such an inquiry may involve requesting information about in-house data security and privacy protections from developers of major COVID-19 contact tracing apps, from data broker firms sharing or selling data to inform public health decisions and research, or from other relevant institutions, such as universities or state and local governments. It may also involve examining laws applicable to the privacy or confidentiality of such data (for example, the Stored Communications Act, HIPAA, and HITECH).
  - The sharing of information between public health experts/officials and law enforcement and immigration agencies, and the consequences of such sharing.

Workers, Laborers, and Hiring – Worker Surveillance and Privacy

- Solicit information from major employers about how their use of technology to mitigate the spread of COVID-19 respects privacy rights of employees, including the collection of biometric information and contact tracing. This initial information request could be followed by a hearing or series of hearings. As appropriate, oversight activities here should include an assessment of compliance with HIPAA and explore the EEOC's efforts to protect worker biometric data.

Additional Priorities – Representation and Diversity in Tech

- Major technology companies continue to have extreme underrepresentation of people of color and women in leadership and engineering roles. This fact is concerning in light of the ways in which algorithms developed by these companies harm underrepresented communities and surveillance tools are used to unfairly track them. Congress should include in its oversight activities efforts to ensure compliance with equal opportunity law and support an inclusive workforce in this key industry. In addition, oversight activity of major technology companies should encourage them to build or sustain civil rights infrastructure within their companies, integrating civil rights expertise at the very highest levels of decision-making.

Census Bureau

Democracy: Voting, the Census, and Hateful Content Online – Census

- Conduct oversight joint hearing with the Census Bureau, FCC, and the Commerce Department on the impacts of an "online-first" census, how the digital divide affected census participation, how the COVID-19 pandemic exacerbated these issues, and the potential impacts of underrepresented communities. This hearing should identify lessons for the 2030 census as well as important research in the intervening years, such as the ACS and the federal data structure in general.

Consumer Financial Protection Bureau

Additional Priorities – Algorithmic Accountability

- Conduct an oversight to ensure that the Consumer Financial Protection Bureau is leading efforts to address bias in artificial intelligence and automated-decision making with respect to the use of AI in banking, insurance, and fintech products.

Department of Commerce

Democracy: Voting, the Census, and Hateful Content Online – Census

- Conduct an oversight joint hearing with the Census Bureau, FCC, and the Commerce Department on the impacts of an "online-first" census, how the digital divide affected census participation, how the COVID-19 pandemic exacerbated these issues, and the potential impacts on underrepresented communities. This hearing should identify lessons for the 2030 census as well as important research in the intervening years, such as the ACS and the federal data structure in general.

Department of Education

Additional Priorities – Algorithmic Accountability

- Conduct oversight to ensure that the Department of Education is leading efforts to address bias in artificial intelligence and automated-decision making with respect to student lotteries, testing accommodations, and admissions practices.

Department of Homeland Security

Policing and Justice – Surveillance of Constitutionally Protected Activity

- Conduct hearings on collaboration and data sharing connected to the implementation of the Department of Homeland Security's Targeted Violence and Terrorism Prevention (TVTP) strategy, including with respect to the surveillance, retention, and dissemination of social media data.

- Conduct hearings on the use of social media by the FBI and the Department of Homeland Security to monitor and track activists and protesters, both historically and in recent months.
  - This exploration should include, but not be limited to, use of social media pursuant to President Trump's executive order and related guidance on protection of statues and monuments.

Policing and Justice – Risk Assessment Tools

- Conduct an oversight hearing examining any technological risk assessment tools being developed or used in support of the Department of Homeland Security's goal of "identify[ing] and respond[ing] to individuals at risk of mobilizing to violence" as part of its broader Targeted Violence and Terrorism Prevention (TVTP) strategy.

Immigration Surveillance Technology – Social Media Monitoring

- Investigate the Department of Homeland Security and the Department of State's invasive and unnecessary programs to collect and monitor social media handles and communications of visitors and immigrants, including U.S. persons. This effort should engage civil society and should focus particularly on the impact of these programs on Muslims and other historically targeted groups; it should also explore the legality of these programs and the likelihood that they are overbroad, ineffective, and discriminatory, while stifling free speech. This oversight effort must include an examination of federal policies and practices applicable to the social media screening of immigrants and travelers and the extent to which those policies and practices are documented and sufficiently thorough, appropriately account for civil rights and liberties concerns, and permit accountability for abuses.

- Request that GAO conduct a review of DHS's and the State Department's collection and use of social media identifiers in connection with the screening of travelers and individuals applying for immigration-related benefits.

Immigration Surveillance Technology – Immigration Surveillance Technology

- Conduct an oversight hearing on DHS's use of invasive surveillance technologies targeting immigrants at the border and in the United States, as well as surveillance of lawyers, journalists, and advocates at the border.

- Conduct an oversight hearing on how DHS and DOJ classify and monitor the activities of groups they categorize as "gangs," including through the maintenance of the Transnational Criminal Organization watchlist. This hearing should examine how this watchlist impacts rights to due process, equal protection, and free association.

- Request a new or updated GAO study of DHS's (including ICE and CBP's) contracting for and purchase of surveillance technology and automated decision-making tools, including those provided by Palantir and other major vendors. To the maximum extent feasible, this study should include an exploration of the use of "off-the-shelf" tools.

Department of Housing and Urban Development

Commercial Data Practices and Privacy – Data Privacy

- Conduct an oversight hearing to hold federal agencies accountable for prioritizing enforcement of existing civil rights laws on online platforms, including in housing and employment. This hearing should include representatives from the DOJ Civil Rights Division, Department of Housing and Urban Development, Department of Labor, and other agencies as appropriate.

Additional Priorities – Disparate Impact

- Congress should conduct an oversight to ensure relevant agencies seek to protect disparate impact standards and apply them appropriately with respect to automated decision-making systems. Requests for information or hearings should explore agency efforts to undermine these rules, such as HUD's recent final rule that makes it easier for landlords to discriminate in housing if they purchase algorithmic screening tools. This oversight should encourage the modification or withdrawal of these rules that facilitate the use of technology to undermine protections long-afforded in cases of disparate impact.

Department of Justice

Additional Priorities – Algorithmic Accountability

- Conduct oversight to ensure that the DOJ is leading efforts to address bias in artificial intelligence and automated-decision making with respect to DNA-matching algorithms.

Immigration Surveillance Technology – Immigration Surveillance Technology

- Conduct an oversight hearing on how DHS and DOJ classify and monitor the activities of groups they categorize as "gangs," including through the maintenance of the Transnational Criminal Organization watchlist. This hearing should examine how this watchlist impacts rights to due process, equal protection, and free association.

Commercial Data Practices and Privacy – Data Privacy

- Conduct an oversight hearing to hold federal agencies accountable for prioritizing enforcement of existing civil rights laws on online platforms, including in housing and employment. This hearing should include representatives from the DOJ Civil Rights Division, Department of Housing and Urban Development, Department of Labor, and other agencies as appropriate.

Department of Labor

Commercial Data Practices and Privacy – Data Privacy

- Conduct oversight hearings to hold federal agencies accountable for prioritizing enforcement of existing civil rights laws on online platforms, including in housing and employment. This hearing should include representatives from the DOJ Civil Rights Division, Department of Housing and Urban Development, Department of Labor, and other agencies as appropriate.

Workers, Labor, and Hiring – Worker Surveillance and Privacy

- Conduct a hearing with relevant Department of Labor leadership to document how it is protecting worker privacy and data using existing legal authorities, including those under Title VII of the Civil Rights Act. This hearing should also include oversight of algorithmic scheduling and management issues.

Department of State

Immigration Surveillance Technology – Social Media Monitoring

- Investigate the Department of Homeland Security and the Department of State's invasive and unnecessary programs to collect and monitor social media handles and communications of visitors and immigrants, including U.S. persons. This effort should engage civil society and should focus particularly on the impact of these programs on Muslims and other historically targeted groups; it should also explore the legality of these programs and the likelihood that they are overbroad, ineffective, and discriminatory, while stifling free speech. This oversight effort must include an examination of federal policies and practices applicable to the social media screening of immigrants and travelers and the extent to which those policies and practices are documented and sufficiently thorough, appropriately account for civil rights and liberties concerns, and permit accountability for abuses.

Equal Employment Opportunity Commission

Workers, Labor, and Hiring – Hiring Assessments

- Conduct a hearing with relevant Equal Employment Opportunity Commission leadership to ensure the agency appropriately prioritizes enforcement of existing nondiscrimination provisions with respect to hiring assessment technologies.

Workers, Labor, and Hiring – Worker Surveillance and Privacy

- Solicit information from major employers about how their use of technology to mitigate the spread of COVID-19 respects privacy rights of employees, including the collection of biometric information and contact tracing. This initial information request could be followed by a hearing or series of hearings. As appropriate, oversight activities here should include an assessment of compliance with HIPAA and explore the EEOC's efforts to protect worker biometric data.

Federal Bureau of Investigation

Policing and Justice – Surveillance of Constitutionally Protected Activity

- Conduct hearings on the use of social media by the FBI and the Department of Homeland Security to monitor and track activists and protestors, both historically and in recent months.
  - This exploration should include, but not be limited to, use of social media pursuant to President Trump's executive order and related guidance on protection of statues and monuments.

Federal Communications Commission

Broadband Internet – Affordable Internet

- Conduct ongoing, robust oversight of the FCC to ensure it is promoting universal affordable broadband by:
  - Improving data collection, including by collecting cost/pricing information, making additional details available to researchers, and continuing efforts to collect more detailed information about coverage areas.
  - Promoting consumer choice by developing standardized disclosures for price and service.
  - Emphasizing effective competition in merger review and regulatory decision-making.
  - Ending harmful efforts to undermine the Lifeline program and moving to strengthen the program and its participation rate.
  - Prioritizing improvements to broadband access and adoption on tribal lands, including through better consultation procedures.

- Demand detailed information from the FCC on its efforts to improve takeup of Lifeline and ensure all eligible participants register and receive benefits.

- Demand the FCC ensure deployment and access on tribal lands be a central element in the commission's annual 706 report and report clearly on the extent to which advanced telecommunications capability is being deployed in a reasonable and timely fashion.

Broadband Internet – Disaster Recovery

- Demand information from the FCC and major ISPs about their disaster response and network interruption procedures with a focus on recent disasters such as Hurricane Maria in Puerto Rico and the California wildfires. This demand for information should include additional data collection about network status during and after disasters by ensuring the FCC requires ISPs submit this data.

Broadband Internet – Wi-Fi and Unlicensed Spectrum

- Push the FCC to open up more unlicensed and shared spectrum to support Wi-Fi, with a focus on current proceedings on the 5.9 and 6 GHz bands.

Broadband Internet – Digital Redlining

- Include questions about efforts to prevent digital redlining in regular FCC oversight hearings.

Democracy: Voting, the Census, and Hateful Content Online – Census

- Conduct an oversight joint hearing with the Census Bureau, FCC, and the Commerce Department on the impacts of an "online-first" census, how the digital divide affected census participation, how the COVID-19 pandemic exacerbated these issues, and the potential impacts on underrepresented communities. This hearing should identify lessons for the 2030 census as well as important research in the intervening years, such as the ACS and the federal data structure in general.

Federal Trade Commission

Commercial Data Practices and Privacy – Data Privacy

- Conduct robust, ongoing oversight of the Federal Trade Commission to ensure it:
  - Investigates, challenges, and punishes abusive commercial data practices, especially with respect to existing consent orders with major technology companies.
  - Invests adequately in expertise on equity and civil rights issues, as well as internal technical capacity, to oversee technology companies.
  - Issues guidance and brings enforcement actions that apply the Unfairness Doctrine to discriminatory practices using a broader understanding of harm.
  - Engages in Magnuson-Moss rulemaking to address commercial data practices.
  - Enforces violations of the Children's Online Privacy Protection Act.

Government Accountability Office

Policing and Justice – Facial Recognition

- Request additional GAO reports on facial recognition as needed to collect further information.

Policing and Justice – Risk Assessment

- Commission a GAO report on the use of risk assessment instruments in federal and state justice systems with a focus on decarceration. Such a study should collect information on:
  - Racial impacts, including practices/processes to ensure racially equitable decarceration.
  - How risks assessments are used (including under what circumstances, by which agencies, and whether they are used independently or in conjunction with other pre-trial systems).
  - What impacts these tools have on release of incarcerated individuals, including specific data on range and incidence of release and conditions as well as analysis of changes in release conditions and outright release.
  - The data from which risk assessments are developed and validated, as well as procedures and frequency for ongoing validation or reassessment efforts.
  - Decision-making frameworks associated with the risk assessment instruments.

Policing and Justice – Law Enforcement Purchase of Location Data and Partnerships with Data Brokers and Other Stakeholders

- Direct the GAO to study federal and state use of private databases and contracting with private companies for law enforcement or surveillance purposes, including, but not limited to Ring, Clearview AI, Sensorvault, and Venntel.

Policing and Justice – Mobile Device Forensic Tools

- Request the GAO produce a study of the tools federal agencies use to extract and analyze information from devices. This study should include exploring the use of federal Regional Computer Forensics Labs, including what technology they use, how it has been validated, what kinds of cases it is being used in, and procedures related to local law enforcement uses of the labs.

Immigration Surveillance Technology – Social Media Monitoring

- Request that GAO conduct a review of DHS's and the State Department's collection and use of social media identifiers in connection with the screening of travelers and individuals applying for immigration-related benefits.

Immigration Surveillance Technology – Immigration Surveillance Technology

- Request a new or updated GAO study of DHS's (including ICE and CBP's) contracting for and purchase of surveillance technology and automated decision-making tools, including those provided by Palantir and other major vendors. To the maximum extent feasible, this study should include an exploration of the use of "off-the-shelf" tools.

Workers, Labor, and Hiring – Hiring Assessments

- Direct the GAO to study:
  - Federal and state government use of hiring assessment technologies.
  - Federal contractor use of hiring assessment technologies.
  - Federal government use of behavioral data collection on employees, decision-making involving such data, and related issues.

The President's Council of Advisors on Science and Technology and the Office of Science and Technology Policy

Policing and Justice – Facial Recognition

- Request the President's Council of Advisors on Science and Technology (PCAST) and the Office of Science and Technology Policy (OSTP) conduct a formal study of the racial bias and due process concerns underlying police use of facial recognition.