ACLU

HARRIS ON SURVEILLANCE

Protecting Individual Liberties and Rights by Constraining Executive Power

Since this nation's founding, the executive branch has been granted — or has claimed — immense power to enforce the law, including the power to surveil, investigate, and impose criminal or other sanctions that deprive individuals of their freedoms. Today, national security agencies in particular — including those with law enforcement, intelligence, homeland security, and defense functions — combine their expansive authorities with unprecedented digital tools that can peer into our personal and professional lives.

Executive branch officials can exercise their powers to surveil and investigate with vast discretion in deciding who to scrutinize, monitor, and pursue through the criminal and civil tools they command. Those decisions can have severe consequences for individual rights. And federal agents can abuse their authority by directing accusations, surveillance, investigations, and prosecutions to target those who dissent against government policies and discriminate against vulnerable communities.

Over the last 20 years and more, the ACLU and our allies have exposed, documented, and challenged abuses that range from Big Brother dragnet surveillance programs to unwarranted and discriminatory domestic surveillance and investigation of protestors, racial and religious minorities, immigrants, and social justice activists. Yet successive presidents — Democrats and Republicans alike — have sought to maintain and dramatically expand executive surveillance powers without meaningful judicial constraints or adequate congressional oversight. Campaign-trail promises to examine and rein in these powers and abuses are all too often broken when the presidential candidate wins office — to the detriment of our system of checks and balances, privacy, civil rights, and civil liberties.

If Vice President Kamala Harris wins the election this November, her administration has the obligation and opportunity to break this cycle. Our roadmap focuses on three core priorities as a start: protecting against Big Brother surveillance; ending unwarranted and discriminatory domestic surveillance and investigation; and implementing strong safeguards for artificial intelligence and data privacy.

OVERALL RESPONSE

The ACLU will push a Harris administration to rein in uses of surveillance that discriminate against people in the United States or invade their privacy; urge the administration and Congress to adopt strong guardrails for the use of artificial intelligence; and challenge executive branch abuses of individual rights and freedoms in court, as we have done throughout our history.

Courts

We will maintain our track record of exposing and challenging federal agencies' infringements of individuals' privacy, civil liberties, and civil rights. We will continue to support and defend protestors, racial and religious minorities, immigrants, and others who are subjected

to abusive surveillance, investigation, prosecution, and coercive measures like wrongful watchlisting. We will seek redress through affirmative litigation when federal agencies abuse their coercive powers in ways that illegally breach Americans' privacy or discriminate based on race, ethnicity, and other protected characteristics.

Congress

Although members of both parties have been quick to empower the executive branch in the name of national and homeland security in the post-9/11 era, we have built a durable bipartisan coalition of advocacy organizations and former and current policymakers to push for limits on government surveillance. We will work with congressional allies to implement specific measures to rein in overbroad and unwarranted surveillance. We will work to change the politics around surveillance and individual liberty, so politicians are more likely to defend our privacy and rights. The ACLU is already responding to current and promised attacks on those who dissent against government policies, and rallying allies around the need for robust separation of powers, strong due process protections, and limits on executive power.

States & Municipalities

We will urge states and cities to restrict the information they provide to federal agencies and departments. For example, the ACLU has successfully advanced state and local laws to increase community control over policing and championed legislation to restrict "reverse" warrants and end purchases of personal information from data brokers. These efforts would reduce the pool of data available to law enforcement, including federal law enforcement. In addition, we will urge state and local governments to end, or sharply limit, their participation in fusion centers and other state-federal intelligence hubs that have been rife with abuse.

SPECIFIC OPPORTUNITIES & RESPONSES

Protecting Against Big Brother Surveillance

The government has vast, unprecedented powers to surveil and peer into people's private lives. It exploits at least three sources to conduct dragnet surveillance of Americans' data: (1) Section 702 of the Foreign Intelligence Surveillance Act (FISA), which authorizes the collection of communications between U.S. persons and people outside the United States; (2) Executive Order 12333, which allows the government to conduct bulk surveillance outside the United States and results in the collection of Americans' private data; and (3) the government's use of commercial data brokers to purchase massive quantities of Americans' private data.[1] Through these dragnet surveillance methods, the federal government obtains access to incredibly sensitive information about Americans — information that can paint a detailed portrait of our private thoughts, relationships, and actions. The government regularly searches through that data for intelligence or domestic law enforcement purposes without a warrant and without notice or other significant safeguards necessary to protect our rights.

For example, the information that the government purchases from data brokers without meaningful oversight and transparency can be highly sensitive, and could include:

- Location information from individuals' visits to health clinics,[2] as well as reproductive tracking applications installed on people's phones;[3]
- Information regarding people's race, ethnicity, gender, sexual orientation, income, and political and religious affiliations;[4] and
- People's immigration status and related information for immigration enforcement.[5]

According to former deputy director of the CIA Michael Morell, "[t]he information that is available commercially would kind of knock your socks off. If we collected it using traditional intelligence methods, it would be top-secret sensitive. And you wouldn't put it in a database, you'd keep it in a safe."[6]

There are few checks on these surveillance powers. Federal agencies rely on them to collect sensitive information without providing a judicial warrant or even notice to individuals whose data has been captured. And the problem is only getting worse as President Biden recently signed legislation dangerously expanding Section 702.[7] Under that expansion, the government can conscript essentially any business that provides Wi-Fi to its customers into service for spying, unless it qualifies for one of Section 702's limited exceptions. The Biden administration has promised it will limit its use of this authority,[8] but that does not commit any future administration to do so.

As a senator, Vice President Harris had a strong track record of legislative efforts to rein in warrantless surveillance of Americans. She served as a member of the Senate Intelligence Committee and voted to require a warrant before law enforcement and intelligence agencies could query Americans' data acquired through Section 702 surveillance. In 2018, she voted "no" on reauthorizing Section 702 because she said it "neglects to adequately protect the privacy rights of the American people."[9] If elected president, Harris will have the opportunity to make good on her commitments to protecting Americans by addressing the long-running harms and privacy violations that result from the government's use of Section 702, Executive Order 12333, and commercial data purchases.

How the ACLU Is Preparing to Respond

Litigation

Because the government uses mass warrantless surveillance authorities (Section 702 of FISA and Executive Order 12333) in secret and without disclosure to the people who are surveilled, it is challenging to identify when someone has been subjected to warrantless surveillance. In practice, people whose privacy rights are violated have had very little legal recourse due to the government's refusal to disclose even basic information about this surveillance and the government's repeated use of the "state secrets privilege" to thwart court review of its most intrusive spying programs. The government used the latter tactic in our lawsuit on behalf of the Wikimedia Foundation and eight other organizations that challenged the National Security Administration's (NSA) Upstream surveillance program, which the government uses to search Americans' internet communications as they enter and leave the country.[10] Even people who are criminally charged at least in part on the basis of evidence derived via Section 702 and Executive Order 12333 are hard-pressed to understand whether and to what extent their private communications have been intercepted and searched.

Although it can be difficult to challenge Section 702 and Executive Order 12333 surveillance, we have done so in the past and will continue to do so by carefully monitoring (1) criminal cases where the government has disclosed its use of other types of sensitive surveillance that are often used in parallel with these secret surveillance methods, (2) publicly available government documents such as Department of Justice (DOJ) press releases, (3) legislative testimony about purported surveillance "successes," and (4) media reports that provide additional information about the government's use of controversial surveillance tools. We will work in collaboration with criminal defense attorneys around the country to file motions that seek to compel the government to provide notice to criminal defendants in investigations where agents relied on Section 702 or Executive Order 12333 surveillance. And in cases where criminal defendants have a basis to believe the government used Section 702 or Executive Order 12333 surveillance to intercept and search their communications without a warrant — as in cases like *United States v. Muhtorov, United States v. Moalin, United States v. Hasbajrami*, and *United States v. Russell*, where we have served as either co-counsel or amicus — we will support defendants in filing motions challenging the lawfulness of that surveillance under the Fourth Amendment and in seeking to suppress the resulting evidence.

By representing defendants who are accused of crimes based on illegally obtained private data, we shed light on the ways in which the government is engaging in mass surveillance of Americans — the vast majority of whom may never know that their privacy has been breached by their government.

Legislative Advocacy

The ACLU has built a durable bipartisan coalition of advocacy organizations and former and current policymakers to push for limits on government surveillance. Before the end of this Congress, the ACLU will continue to work with congressional allies to narrow the recent expansion of the definition of "electronic communications service providers" that would allow the government to force a wide range of U.S. businesses to give the NSA access to their Wi-Fi routers, phones, and other communications equipment.[11] As a part of this process, the ACLU will also work to reverse the changes made under this year's reauthorization that weaken the FISA Court's ability to obtain independent input from experts on civil rights, civil liberties, and privacy when the government secretly seeks permission to conduct novel forms of surveillance.

Looking forward, given that Congress only reauthorized Section 702 for two years, there will be another opportunity by April 2026 to address the ACLU's longstanding concerns regarding mass warrantless surveillance. We will continue to work with the bipartisan surveillance coalition to limit the federal government's vast ability to search Americans' private communications without a warrant, whether with Section 702, Executive Order 12333, or the purchase of data the government would otherwise need a warrant to obtain. For instance, this year, the ACLU and allies successfully advocated for House passage on a wide bipartisan basis of the Fourth Amendment Is Not For Sale Act, a bill that would prevent the government from purchasing data that would otherwise require a warrant to obtain, although the Senate failed to pass an amendment to the same effect as part of the Section 702 reauthorization law.[12] The ACLU will continue to build up support for this legislation to get it passed in the Senate and will encourage Harris to sign it if she is in the White House. Depending on the outcome of the November election and the composition of the

congressional oversight committees, we will also work to ensure that Congress conducts vigorous oversight over the government's surveillance powers and practices.

Local & State Advocacy

In addition, the ACLU will urge states and cities to restrict the information they provide to federal agencies and departments. For example, the ACLU has successfully advanced state and local laws to increase community control over policing and championed legislation to restrict "reverse" warrants and end purchases of personal information from data brokers.[13] These efforts would reduce the pool of data available to law enforcement, including federal law enforcement. In addition, the ACLU will urge state and local government to end, or sharply limit, their participation in fusion centers and other state-federal data sharing arrangements that have been rife with abuse.

Ending Unwarranted and Discriminatory Domestic Surveillance and Investigation

Domestic national security and counterterrorism policies and programs pose a singular threat to Americans' privacy, civil rights, and civil liberties. Taken as a whole, these policies reflect: the federal government's expansive claimed authority to surveil and monitor American communities;[14] federal nondiscrimination guidance that permits profiling on the basis of race, religion, national origin, and other protected characteristics;[15] and the use of overbroad and unfair programs such as the watchlisting system, or tools like social media surveillance, against people exercising constitutionally protected speech and association rights.[16]

Federal agencies exercise their authority and wield technology to disproportionately and wrongly surveil and investigate, watchlist, question, and detain at the border, and deny immigration benefits to vulnerable communities. Even when federal surveillance and investigation policies appear facially neutral, in practice, for the past 20 years — and longer — Democratic and Republican administrations alike have disproportionately targeted those who dissent against government policies, racial and religious minorities, and immigrant communities through the lens of "security threat" or "risk,"[17] and undermined our rights to free expression, due process, religious freedom, and equal protection under the law.[18] The harsh reality is that federal national security surveillance and investigation discriminate against communities of color in this country, denying their ability to participate as equals in civic life and our democracy. A Harris administration urgently needs to rein in and reform key overbroad, unnecessary, and discriminatory domestic surveillance policies and programs.

Federal law enforcement and intelligence agencies' use of national security investigative authorities flows in part from the USA Patriot Act of 2001, which enacted — for the first time — a definition of "domestic terrorism." That definition is vague, overbroad, and malleable, covering acts deemed "dangerous to life" that "appear to be intended to" intimidate or coerce the public or the government.[19] It is increasingly being copied by state legislatures.[20] Law enforcement and intelligence agencies have used this definition to claim expansive investigative authorities. For example, soon after Congress passed the Patriot Act, the DOJ loosened safeguards intended to protect Americans against intrusive FBI surveillance and investigation.[21] FBI agents can now open "assessments" without any factual basis for suspicion of actual criminal wrongdoing,[22] and use invasive techniques for data gathering, such as racial and ethnic mapping, confidential informants, physical surveillance, and commercial and law enforcement database searches.[23]

Recent history is rife with federal agencies' use of these and similar authorities to unfairly target people of color and other marginalized communities for surveillance, investigation, prosecution, and placement on watchlists. For example:

- The FBI has spied on Muslim communities and, more generally, treated nonviolent civil disobedience and vandalism as justification for conducting national security investigations of civil rights, social justice, and environmental activists; [24]
- In 2020, the DOJ deployed joint federal-state law enforcement partnerships to conduct "counterterrorism" investigations against racial justice protestors; [25] and
- The Department of Homeland Security (DHS) has all too often focused its surveillance authorities on political and constitutionally protected speech, as well as activities far outside its homeland security mandate, including those of: journalists; racial justice demonstrators in the wake of George Floyd's murder; and people simply reacting online to the Supreme Court's decision to overturn *Roe v. Wade*. The DHS has also conducted other social media monitoring that bases inquiries on commonly held political views.[26]

It's long past time for reforms, including, in particular, banning biased profiling and investigations through strong agency policy prohibitions without any loopholes for national and homeland security. Indeed, President Biden raised hopes when he directed the DOJ and DHS to "assess the implementation and effects" of the Justice Department's 2014 Guidance on Race, which has long been shown to permit bias, to "consider whether this guidance should be updated."[27] But to our disappointment,

when the DOJ updated this guidance in 2023, it kept in place the broad loopholes permitting racial, religious, and other biases in the contexts of national and homeland security and immigration.[28]

The DHS has adopted the 2023 DOJ Guidance on Race in part, while it considers further updates of department nondiscrimination policy.[29] By virtue of its far-reaching mandate and numerous component agencies, the DHS is the face of federal law enforcement and surveillance power for vastly more people than the DOJ. Its nondiscrimination policies permit bias-based profiling in the national security context, at the border, and in protective, inspection, or screening activities. The DHS's extensive surveillance tools include social media monitoring; purchases of commercial datasets that can include sensitive location information; collection of biometric information at ports of entry; and the monitoring of passenger travel records, which are then mined to conduct even more intrusive physical and electronic searches when individuals are crossing the border. The resulting data is processed and distributed by a sprawling web of interconnected systems, which inform or guide agency decisions affecting individuals' privacy and basic civil rights and civil liberties. Together, expansive claims of investigative powers and gravely inadequate safeguards facilitate abusive approaches across a range of DHS policies, programs, and subcomponents. For example, in recent years, DHS-supported fusion centers, which are joint federal-state surveillance hubs, have monitored protesters at Standing Rock, people protesting the Trump administration's family separation and border policies, and Black Lives Matter activists.[30]

How the ACLU is Preparing to Respond

Ending discriminatory surveillance through litigation and advocacy. As we have over the last 20 years and more, we will ensure transparency and accountability for unwarranted and discriminatory surveillance through litigation in federal and state courts. For example, in July 2024, we sued to force disclosure of DOJ and DHS records on federal-state law enforcement and intelligence hubs that have long been used to surveil protestors and communities of color, in order to assess their impact on privacy and rights during both the Trump and Biden administrations.[31] Working alongside impacted communities and allies, we will also urge a Harris administration to end biased national and homeland security profiling by federal, state, and local law enforcement. While President Biden has been willing to countenance biased DOJ and DHS surveillance and investigation policies, a Harris administration should recognize not only historical and current harms, but also the significant risks to Americans from future administrations with even less regard for privacy, civil rights, and civil liberties.

The ACLU will advocate with a Harris administration for DOJ and DHS nondiscrimination policies that: (1) explicitly prohibit discrimination based on actual or perceived race, ethnicity, religion, national origin and nationality, sexual orientation, and gender (including gender identity and expression), without any loopholes for national and homeland security; (2) ensure that a person's nationality and national origin are not used as a proxy to discriminate against them based on their religion, race, or ethnicity; (3) applies these safeguards to state and local agencies that participate in joint operations or partnerships with the DOJ and/or DHS; and (4) require a rigorous and systematic audit of each department's programs and operations for bias based on the use of protected characteristics.

Ending discriminatory, unfair, and secretive watchlisting through litigation and advocacy. The ACLU and our allies have documented and raised grave concerns about the discriminatory, unfair, and secretive U.S. watchlisting system for two decades, including highlighting its use as a tool for continued investigation and coercive pressure on Americans to become informants on their communities. Through litigation on behalf of our American Muslim clients, we forced the government to change its No Fly List redress program so that it now discloses to Americans whether they are on the No Fly List, as well the criteria it uses for that placement,[32] but these changes are far from adequate and we will continue to challenge wrongful placement of Americans on the No Fly List in court in order to achieve systemic reform.

At the same time, the U.S. federal watchlist system as a whole continues to be a black box and has now ballooned dramatically to 2 million people.[33] American Muslims and those of Arab, Middle Eastern, or South Asian descent are disproportionately watchlisted[34] and suffer the brunt of the stigmatizing and devastating personal and professional consequences. These consequences flow in part from the fact that the government shares watchlisting records with at least 60 foreign governments and numerous private entities;[35] government agencies that perform screening functions (such as the Transportation Security Administration, Customs and Border Patrol, and U.S. Citizenship and Immigration Services); and tens of thousands of state, local, and tribal law enforcement agencies nationwide.[36] For U.S. persons, this can mean detention and questioning by other governments while abroad; potentially unlawful searches, seizures, and surveillance;[37] inability to open or maintain bank accounts; denial of government licenses or employment; and indefinite delays or denials of immigration benefits.

The executive branch exercises virtually unfettered discretion in deciding whom to watchlist, using vague and overbroad criteria and a low bar for placement. Its redress process is a due process nightmare, denying Americans meaningful notice and an opportunity to challenge wrongful watchlisting. If our government is to have a watchlisting system, a Harris administration needs to ensure meaningful redress, requiring at a minimum:

- disclosure of watchlisting status to all U.S. persons, and not only to U.S. persons on the No Fly List;
- disclosure to U.S. persons of the specific criteria or criterion under which they are watchlisted; all reasons that they, in the government's view, meet those criteria; and all material inculpatory and exculpatory evidence. Disclosures must be consistent with due process and, to the extent that legitimately classified information is used as a basis for determination, the government should apply standards under 8 C.F.R. § 103.2(b)(16);
- prompt and public time limits for responding to redress applicants at each stage of the process;
- a live hearing before a neutral decision-maker in which a wrongly watchlisted U.S. person may fully and fairly present their case.

Ending discriminatory and ineffective collection and monitoring of social media information through transparency litigation and advocacy. Through transparency litigation, we forced disclosure of federal agencies' monitoring of social media users and speech, exposing the dangers of surveillance without any suspicion of criminal wrongdoing.[38] Our focus has included agencies' collection of social media identifiers from visa applicants seeking leave to enter the United States, which gives the government sweeping access into visa applicants' online lives, as well as the lives of people in the United States with whom they interact. This poses acute risks[39] for people from Muslim countries and their American family, friends, and colleagues. More broadly, social media monitoring programs easily allow the targeting of political and religious beliefs. This fear is particularly pronounced in the current environment of protests on social media and the streets against the war in Gaza. Indeed, since October 7, 2023, there have been reports of CBP asking Palestinians about their social media posts and of U.S. residents being contacted by federal agents asking about their social media posts, perhaps at the request of the social media companies.[40] Social media is notoriously difficult to interpret, and agencies often wrongly interpret posts as threatening or assume political and religious views are connected with violence.[41]

Since 2016, government officials and entities have raised questions about whether this type of screening helps weed out genuine security concerns.[42] A 2021 analysis of social media collection by the Office of the Director of National Intelligence said the collection of identifiers added "no value" to the accuracy of immigration screening and vetting programs, with a senior administration official confirming that "collecting social media data had yet to identify terrorists among visa applicants."[43]

Given the known risks of these programs, the lack of evidence of their utility, and their disparate use and impact, we will continue to litigate and advocate with a Harris administration to end these programs and purge all information they have generated unless it is relevant to an ongoing criminal investigation.

Implementing Strong Safeguards for Artificial Intelligence and Data Privacy

The federal government's use of artificial intelligence (AI) urgently needs greater oversight and stronger safeguards to protect our privacy. Federal agencies of all stripes are using algorithmic systems and AI to make adjudicatory and policy decisions that were once reserved for human decisionmakers. The use of AI for those critical decisions spans all aspects of the government, including determining public benefits levels, assessing families for child welfare proceedings, scoring incarcerated individuals for early release, and identifying individuals for criminal investigations.[44] These uses carry risks for civil rights and civil liberties, including in chilling the exercise of the right to speak or protest; moreover, many uses of AI have been well documented to lead to arbitrary and even discriminatory outcomes.

National security agencies — including those with law enforcement, intelligence, homeland security, and defense components — have long relied on AI systems and are rapidly expanding their use, presenting immense risks to the rights and safety of people in the United States and abroad. While Congress and the Biden-Harris administration have taken steps to increase transparency, trust, and fairness in the AI tools used by many federal agencies, national security agencies have been largely exempted from these important measures. Indeed, U.S. national security agencies and the military are seeking to integrate AI into some of the government's most profound decisions, including: who it surveils; who it places on government watchlists; who it subjects to intrusive searches at the border; who it labels a "risk" or "threat" to national security; and even who or what it targets with

lethal force. These programs have not been meaningfully tested for efficacy and are characterized by vague and overbroad standards, weak safeguards, and little to no transparency.

Despite the dangers these national security systems pose, they lack any meaningful transparency and accountability safeguards — and, to the extent protections exist at all, they are largely unenforceable. The public knows little about the AI being deployed by the country's largest intelligence, homeland security, and law enforcement entities like the DHS, FBI, NSA, and CIA. And the public knows even less about the civil rights and liberties protections that exist — if any. National security agencies have embarked on an all-out sprint to develop and deploy AI, but any efforts to protect privacy, civil rights, and civil liberties have been slow-moving and without binding rules.

As Vice President Harris recognized when the White House announced its Executive Order on AI, "We have a moral, ethical and societal duty to make sure that A.I. is adopted and advanced in a way that protects the public from potential harm and ensures that everyone is able to enjoy its benefits."[45] If Harris is elected president, her administration should ensure that strong baseline protections for AI apply to national security and non-national security uses alike.

More broadly, the federal government must also take significant steps to protect our sensitive data from being bought, sold, and exploited by tech companies and government agencies alike to learn private facts about our lives.

How the ACLU is Preparing to Respond

Executive Branch & Legislative Advocacy on AI

Under a Harris administration, federal agencies should establish robust safeguards around the federal uses of AI that impact rights and safety. Those safeguards should apply where AI affects individuals' rights in our day-to-day lives including freedom of speech, education, employment, credit, housing, immigration, the criminal legal system, and more.[46] Federal agencies should subject their use of rights- and safety-impacting AI to certain minimum safeguards, including: impact assessments that gauge the risks posed by AI; testing AI in a real-world context; mitigating harms including discrimination; and discontinuing use of the AI where the harms may not be adequately mitigated.[47] Other safeguards should include increased transparency about where AI is used and for what purposes; independent evaluations of the AI's performance; ongoing monitoring for harms; and engaging impacted communities on AI use and impact. Many of these safeguards are already embodied in President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[48] A Harris administration should build on Vice President Harris's leadership and continue advancing the Executive Order.[49]

When it comes to the use of AI by national security agencies, we will advocate for far stronger executive branch and legislative protections. While the rushed adoption of AI poses risks in many contexts, the use of AI for counterterrorism and other national security programs and policies presents some of the greatest dangers to people in the United States and abroad. The deployment of AI systems for surveillance, watchlisting, border searches, biometric identification, and immigration vetting will automate, expand, and make even more opaque some of the government's most intrusive, damaging, and secretive programs. Moreover, these programs and activities disproportionately impact communities that have long faced bias and discrimination, such as immigrants and racial and religious minorities. As in areas like policing and the criminal legal system, without strong safeguards, the use of AI for national security purposes can easily perpetuate racial, ethnic, or religious profiling, while broadly endangering civil rights and civil liberties.

Because of these dangers, the ACLU will press a Harris administration to urgently adopt safeguards that include: (1) increased transparency across "national security systems" that rely on AI, through the development of comprehensive AI use case inventories, regular declassification reviews, and improvements in existing transparency reporting; (2) adoption of risk management practices that reduce or prevent harm to privacy and civil liberties, including impact assessments, real-world testing, and ongoing risk monitoring protocols; (3) increased scrutiny and oversight of whether and to what extent AI has been effective at accomplishing the agency's counterterrorism or national security objectives, such as through meaningful gains in the accuracy of detecting or preventing terrorism activities; (4) a minimum standard requiring agencies to refrain from or cease AI use when the AI is not sufficiently tested; it is unreliable or otherwise ineffective; or it raises risks to privacy, civil liberties, civil rights, or safety that cannot be effectively mitigated; and (5) increased resources and support for agencies' internal oversight mechanisms to scrutinize and ensure compliance with AI-related safeguards.[50]

Transparency Litigation in the Courts

We will litigate Freedom of Information Act (FOIA) lawsuits seeking to ensure greater public transparency about the use of AI for national security purposes.

For example, the ACLU has filed FOIA requests seeking records about the NSA's use of AI to conduct surveillance. Among U.S. intelligence agencies, the NSA is the self-described leader in the race to develop and deploy AI.[51] According to officials, the NSA has used AI "for a very

long time" to support its intelligence-gathering activities, and today it is one of many spy agencies seeking to integrate AI across its activities.[52] Yet the public knows very little about how exactly the agency is harnessing AI. NSA officials have publicly described the agency's use of AI tools to detect threats to critical infrastructure, to summarize large amounts of information or raw intelligence, and to perform "speaker identification and speech-to-text processing."[53] The NSA likely also uses these tools to select new surveillance targets and to analyze the vast amounts of communications it collects every day — often ensnaring people in the United States.[54] Indeed, although the NSA generally seeks to collect foreign intelligence, the mass surveillance it conducts under Section 702 of FISA and other authorities like Executive Order 12333 routinely sweeps up the sensitive communications and data of Americans.[55] Yet little is known about the efficacy of the NSA's AI tools, or what safeguards for civil rights and civil liberties are in place.

Similarly, the ACLU has filed FOIA requests seeking records about the DHS's use of AI to conduct risk assessments of people seeking to enter, leave, or travel within the United States. CBP today uses "machine learning" to conduct risk assessments of travelers at U.S. ports of entry.[56] In producing these risk assessments, CBP applies machine learning to its data holdings — which include information from dozens of databases from federal, state, and local governments, as well as from private brokers, amassed within the DHS's notoriously opaque Automated Targeting System (ATS).[57] CBP uses ATS to apply "risk-based rules based on CBP officer expertise, analysis of trends of suspicious activity, and raw intelligence from DHS and other government agencies to assist CBP officers in identifying individuals who require additional inspection or in determining whether individuals should be allowed or denied entry into the United States."[58] The TSA also relies on ATS and related databases to conduct its own rules-based risk assessments. Passengers flagged under the rules may be subject to more intrusive screening.[59] Yet the public knows almost nothing about the AI systems CBP and the TSA use to conduct these rules-based risk assessments, including how the agencies select and train the models they rely upon, how the agencies assess the systems' performance, and what measures the agencies have taken to ensure our privacy and other rights are protected.

The government's lack of transparency is especially concerning given the danger that many AI systems pose for people's privacy and civil rights and civil liberties. Just as in areas like law enforcement, using algorithmic systems to gather and analyze intelligence can compound privacy intrusions and perpetuate discrimination. AI systems may amplify biases that are embedded in the datasets used to train those systems, and they may have higher error rates when applied to people of color and marginalized communities because of flaws in the algorithms or underlying data. AI-driven surveillance may be used to guide or expand government activities that have long been used to unfairly scrutinize communities of color. For example, built-in bias or flawed intelligence algorithms may lead to additional unwarranted surveillance and investigation of individuals, exposing their lives to wide-ranging government scrutiny under FISA or other authorities.

We will pursue litigation where necessary to compel national security agencies to promptly process our FOIA requests, search their files for responsive records, and produce the resulting documents to the ACLU for public dissemination and advocacy for necessary reforms. Where agencies withhold responsive records or information on national security or other grounds, we will consider further litigation seeking to pry critical information loose. Only with greater transparency can we ensure that the public and Congress have the information they need to oversee these society-altering systems.

Legislative Advocacy on a Federal Comprehensive Privacy Law

The amount of data that is available to national security agencies — including commercially available data — may also be addressed through a federal comprehensive privacy law. The goal of privacy legislation should be to reduce the amount of data that is being collected from us in the first place and — consistent with the First Amendment — reduce its downstream use, sharing, and retention. Key to achieving these goals are four requirements.[60] First, data minimization would require that entities limit their collection, use, and disclosure of data to what is necessary to provide services requested by consumers — including by limiting sales to national security agencies. Second, civil rights protections should prohibit discriminatory uses of data.[61] And third and fourth, a robust federal privacy law should provide individuals with a private right of action and limit preemption of state and local laws by setting a "floor" that states and municipalities may build upon.[62] In addition to advocating for new legislation, the ACLU will seek to vigorously encourage the use of congressional oversight hearings on the civil liberties implications of increased use of AI.

CONCLUSION

The federal government's power to surveil, investigate, prosecute, and intimidate is vast — and Democratic administrations, like Republican ones, have a pattern of defending executive power at the expense of individual freedoms and rights. But the ACLU exists to ensure those powers are constrained and abuses are challenged. If elected, Harris will face both tests and opportunities for significant surveillance reforms to safeguard our privacy and constrain policies and programs that already undermine civil liberties and rights. As we have for over a century, the ACLU will use every tool at our disposal — in the courts, in Congress, and in the halls of power in states and cities — to uphold our system of checks and balances, safeguard privacy, and enforce the protections of the Bill of Rights for all.

ENDNOTES

1 Law enforcement and intelligence agencies that have purchased cellphone location data include the FBI, the Drug Enforcement Administration, Immigration and Customs Enforcement, Customs and Border Protection, the Secret Service, the Department of Homeland Security, and the Department of Defense.

2 Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, Vice (May 3, 2022), https://www.vice.com/en/article/location-data-abortion-clinics-safegraph-planned-parenthood/

3 Joseph Cox, *Data Marketplace Selling Info About Who Uses Period Tracking Apps*, Vice (May 17, 2022), https://www.vice.com/en/article/data-marketplace-selling-clue-period-tracking-data/.

4 Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), https://www.vice.com/en/article/us-military-location-data-xmode-locate-x/#:~:text=The%20other%20stream%20is%20through,and%20by%20extension%2C%20the%20military.

5 Joan Friedland, *How the Trump Deportation Machine Relies on Inaccurate Databases and Unregulated Data Collection*, Nat'l Immigr. L. Ctr. (Nov. 1, 2019), https://www.nilc.org/2019/11/01/inaccurate-data-unregulated-collection-fuel-deportation-machine/

6 Byron Tau, *U.S. Spy Agencies Know Your Secrets. They Bought Them.*, Wall St. J. (Mar. 8, 2024), https://www.wsj.com/politics/national-security/u-s-spy-agencies-know-our-secrets-they-bought-them-791e243f

7 50 U.S.C. § 1881a.

8 According to the New York Times, one of the purposes of this provision was to address a Foreign Intelligence Surveillance Court (FISC) decision holding that data centers for cloud computing did not qualify as "electronic communication service providers." Charlie Savage, *Secret Rift Over Data Center Fueled Push to Expand Reach of Surveillance Program,* N.Y. Times (Apr. 16, 2024), https://www.nytimes.com/2024/04/16/us/fisa-surveillance-bill-program.html. Although Senator Warner, the chairman of the Intelligence Committee, has stated that he supports narrowing this provision further as part of the Intelligence Authorization Act, it remains to be seen if Congress will act to do so before the end of this year.

9 Vice President Harris's running mate Governor Tim Walz also had a similar recording during his time in the House. He voted against enactment of Section 702 in 2008 and voted no on reauthorization in both 2012 and 2018. He further voted to close the backdoor search loophole in both 2015 and 2016 and for the USA Rights Act amendment in 2018 that would have also closed the backdoor search loophole.

10 *Wikimedia v. NSA - Challenge to Upstream Surveillance*, ACLU, https://www.aclu.org/cases/wikimedia-v-nsa-challenge-upstream-surveillance (last updated Feb. 21, 2023).

11 Press Release, ACLU, Despite Bipartisan Outcry, Senate Betrays the Fourth Amendment and Passes Bill to Expand Warrantless Government Surveillance (Apr. 20, 2024), https://www.aclu.org/press-releases/senate-reauthorizes-and-expands-section-702-surveillance.

12 *Id.*

13 *See Privacy & Technology*, ACLU, https://www.aclu.org/issues/privacy-technology (last visited Aug. 25, 2024).

14 *Surveillance Under the USA/Patriot Act*, ACLU (Oct. 23, 2002), https://www.aclu.org/other/surveillance-under-usapatriot-act.

15 U.S. Dep't of Justice, Guidance for Fed. Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity (Dec. 2014), https://www.dhs.gov/sites/default/files/publications/use-of-race-policy_0.pdf.

16 Hugh Handeyside, *The Watchlisting System Exemplifies the Government's Post-9/11 Embrace of Biased Profiling*, ACLU (Sept. 9, 2021), https://www.aclu.org/news/national-security/the-watchlisting-system-exemplifies-the-governments-post-9-11-embrace-of-biased-profiling.

17 Hum. Rts. Watch, Illusion of Justice: Human Rights Abuses in US Terrorism Prosecutions (July 2014), https://www.hrw.org/report/2014/07/21/illusion-justice/human-rights-abuses-us-terrorism-prosecutions.

18 *Top Ten Abuses of Power Since 9/11*, ACLU (Sept. 6, 2006), https://www.aclu.org/other/top-ten-abuses-power-911.

19 USA Patriot Act, Pub. L. No. 107–56, § 802, 115 Stat. 376 (2001) (codified as amended at 18 U.S.C. § 2331).

20 *State Domestic Terrorism Laws in the United States*, Internat'l Ctr. for Not-For-Profit L., https://www.icnl.org/resources/terrorism-laws-in-the-united-states (last updated Mar. 7, 2024).

21 ACLU, Unleashed and Unaccountable: The FBI's Unchecked Abuse of Authority 9–15 (Sept. 2013), https://www.aclu.org/sites/default/files/field_document/unleashed-and-unaccountable-fbi-report.pdf.

22 *See* Fed. Bureau of Investigation, Domestic Investigations and Operations Guide §§ 4.3.3, 5.1, 6.5–6 (Mar. 2016), https://www.justsecurity.org/wp-content/uploads/2019/03/FBI.DIOG_.pdf.

23 *See, e.g., id.* at § 4.3.3; ACLU, Expanded FBI Authority (Oct. 19, 2011), https://www.aclu.org/other/expanded-fbi-authority (explaining expanded FBI authorities and recommended reforms).

24 *See generally* ACLU, Unleashed and Unaccountable: The FBI's Unchecked Abuse of Authority 9–15 (Sept. 2013), https://www.aclu.org/sites/default/files/field_document/unleashed-and-unaccountable-fbi-report.pdf. *See also* Press Release, ACLU, New Documents Show FBI Targeting Environmental and Animal Rights Groups Activities as 'Domestic Terrorism' (Dec. 20, 2005), https://www.aclu.org/news/new-documents-show-fbi-targeting-environmental-and-animal-rights-groups-activities-domestic; Janet Reitman, *I Helped Destroy People*, N.Y. Times (Sept. 1, 2021), https://www.nytimes.com/2021/09/01/magazine/fbi-terrorism-terry-albury.html.

25 Press Release, DOJ, Att'y Gen. William P. Barr's Statement on Riots and Domestic Terrorism (May 31, 2020), https://www.justice.gov/opa/pr/attorney-general-william-p-barrs-statement-riots-and-domestic-terrorism.

26 *Gill v. DOJ – Challenge to Government's Suspicious Activity Reporting Program,* ACLU (July 11, 2014), https://www.aclu.org/cases/gill-v-doj-challenge-governments-suspicious-activity-reporting-program; Shane Harris, *DHS Compiled "Intelligence Reports" on Journalists Who Published Leaked Documents*, Washington Post, July 30, 2020, https://www.washingtonpost.com/national-security/dhs-compiled-intelligence-reports-on-journalists-who-published-leaked-documents/2020/07/30/5be5ec9e-d25b-11ea-9038-af089b63ac21_story.html; Press Release, Ron Wyden, Wyden Releases New Details About Surveillance and Interrogation of Portland Demonstrators by Department of Homeland Security Agents (Oct. 27, 2022), https://www.wyden.senate.gov/news/press-releases/wyden-releases-new-details-about-surveillance-and-interrogation-of-portland-demonstrators-by-department-of-homeland-security-agents; *DHS monitored 'social media reactions' to Roe, collected legally protected speech, bulletin shows*, Yahoo News, (Nov. 16, 2022), https://www.yahoo.com/news/dhs-monitored-social-media-reactions-to-roe-collected-legally-protected-speech-bulletin-shows-001254616.html.; *Homeland Security Considers Outside Firms to Analyze Social Media After Jan. 6 Failure*, Wall Street J., Aug. 15, 2021, https://www.wsj.com/articles/homeland-security-considers-outside-firms-to-analyze-social-media-after-jan-6-failure-11629025200.

27 Press Release, White House, Executive Order on Advancing Effective, Accountable Policing and Criminal Justice Practices to Enhance Public Trust and Public Safety (May 25, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/05/25/executive-order-on-advancing-effective-accountable-policing-and-criminal-justice-practices-to-enhance-public-trust-and-public-safety/.

28 ACLU et al., Concerns about the Department of Justice's 2023 Racial Profiling Guidance (2023).

29 Pol'y Statement 500-02 to Dep't Homeland Sec. Agency and Office Leaders from Sec'y Alejandro Mayorkas on Reaffirming the Commitment to Nondiscrimination in Dep't of Homeland Sec. Activities (May 25, 2023), https://www.dhs.gov/sites/default/files/2023-06/2023.05.25_S1_Policy%20Statement%20500-02_Reaffirming%20DHS%20Commitment%20to%20Nondiscrimination_508.pdf.

30 *See* Alleen Brown, Will Parrish & Alice Speri, *Standing Rock Documents Expose Inner Workings of "Surveillance-Industrial Complex,"* Intercept (June 3, 2017), https://theintercept.com/2017/06/03/standing-rock-documents-expose-inner-workings-of-surveillance-industrial-complex; Ryan Devereaux, *Homeland Security Used a Private Intelligence Firm to Monitor Family Separation Protests,* Intercept (Apr. 29, 2019), https://theintercept.com/2019/04/29/family-separation-protests-surveillance; George Joseph, *Exclusive: Feds Regularly Monitored Black Lives Matter Since Ferguson*, Intercept (July 24, 2015), https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson.

31 *ACLU v. DOJ – FOIA Lawsuit Seeking Records About the Use of JTTFs and Fusion Centers to Target Protestors and Communities of Color*, ACLU (July 29, 2024), https://www.aclu.org/cases/aclu-v-doj-foia-lawsuit-seeking-records-about-the-use-of-jttfs-and-fusion-centers-to-target-protesters-and-communities-of-color.

32 *Kashem, et al. v. Barr, et al. - ACLU Challenge to Government No Fly List*, ACLU (Apr. 7, 2021), https://www.aclu.org/cases/kashem-et-al-v-barr-et-al-aclu-challenge-government-no-fly-list.

33 E.D. Cauchi & Imtiaz Tyab, *U.S. terrorist watchlist grows to 2 million people — nearly doubling in 6 years*, CBS News (Dec. 14, 2023), https://www.cbsnews.com/news/us-terrorist-watchlist-grows/.

34 *Id.*

35 *Elhady v. Kable*, No. 16-cv-375 (E.D. Va. Mar. 12, 2019).

36 Homeland Sec. & Gov. Sec., Mislabeled as a Threat: How the Terrorist Watchlist & Government Screening Practices Impact Americans 31–32 (Dec. 2023), https://www.hsgac.senate.gov/wp-content/uploads/Mislabeled-as-a-Threat_Public_Report-2.pdf.

37 Elhady at 46-48; *See also Latif v. Lynch*, No. 10-cv-00750 (D. Or. Aug. 7, 2015); *Meshal v. Wright*, 651 F. Supp. 3d 1273 (S.D. Ga. 2022).

38 Shaiba Rather & Layla Al, *Is the Government Tracking Your Social Media Activity?*, ACLU (Apr. 24, 2023), https://www.aclu.org/news/national-security/is-the-government-tracking-your-social-media-activity.

39 Karen Zraick & Mihir Zaveri, *Harvard student says he was barred from U.S. over his friends' social media posts,* The New York Times (Aug. 27, 2019), https://www.nytimes.com/2019/08/27/us/harvard-student-ismail-ajjawi.html.

40 Hannah Allam, *How the FBI's visit to a Muslim woman became a right-wing rallying cry*, Wash. Post (Apr. 1, 2024), https://www.washingtonpost.com/national-security/2024/03/31/fbi-oklahoma-social-media-gaza/.

41 The numerous comments submitted by the Brennan Center and other civil society organizations in response to requests for notice and comment from the Departments of State and Homeland Security regarding collection and use of social media have detailed these concerns and others. *See Timeline of Social Media Monitoring for Vetting by the Department of Homeland Security and the State Department*, Brennan Ctr. for Justice, https://www.brennancenter.org/our-work/research-reports/timeline-social-media-monitoring-vetting-department-homeland-security-and (last updated Dec. 21, 2023).

42 U.S. Citizenship and Immigr. Servs., DHS Sec'y Briefing Binder 181 (2016), https://www.dhs.gov/sites/default/files/publications/USCIS%20Presidential%20Transition%20Records.pdf (noting that the Fraud Detection and National Security Directorate within USCIS "encountered a number of challenges, limitations, and inefficiencies" while testing a social media screening tool and "concluded that [the tool] did not meet USCIS needs for social media screening"); Off. of Inspector Gen., No. OIG-17-40, DHS' Pilots for Social Media Screening Need Increased Rigor to Ensure Scalability and Long-term Success (Feb. 27, 2017), https://www.oig.dhs.gov/sites/default/files/assets/2017/OIG-17-40-Feb17.pdf.

43 Charlie Savage, *Visa applicants' social media data doesn't help screen for terrorism, documents show* N.Y. Times (Oct. 5, 2023), https://www.nytimes.com/2023/10/05/us/social-media-screening-visa-terrorism.html.

44 Letter from ACLU to Off. of Mgmt. & Budget 12-15 (Dec. 5, 2023), https://www.aclu.org/documents/aclu-encourages-omb-to-provide-robust-protections-for-civil-rights-and-civil-liberties-in-government-uses-of-ai.

45 David McCabe & Cecilia Kang, *A Kamala Harris Presidency Could Mean More of the Same on A.I. Regulation*, N.Y. Times (July 24, 2024), https://www.nytimes.com/2024/07/24/technology/kamala-harris-ai-regulation.html.

46 Letter from ACLU to Off. of Mgmt. & Budget 12-15 (Dec. 5, 2023), https://www.aclu.org/documents/aclu-encourages-omb-to-provide-robust-protections-for-civil-rights-and-civil-liberties-in-government-uses-of-ai.

47 *Id*. at 15-26.

48 Exec. Order No. 14110, 88 C.F.R. 75191 (Nov. 1, 2023).

49 Press Release, White House, Remarks by Vice President Harris on the Future of Artificial Intelligence (Nov. 1, 2023), https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/11/01/remarks-by-vice-president-harris-on-the-future-of-artificial-intelligence-london-united-kingdom/; Press Release, White House, Fact Sheet: Vice President Harris Announces New U.S. Initiatives to Advance the Safe and Responsible Use of Artificial Intelligence (Nov. 1, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/fact-sheet-vice-president-harris-announces-new-u-s-initiatives-to-advance-the-safe-and-responsible-use-of-artificial-intelligence/.

50 *See* Letter from the ACLU & Brennan Ctr. for Just. to Priv. & Civ. Liberties Oversight Bd. (July 1, 2024), https://www.aclu.org/documents/aclu-brennan-pclob-ai-review.

51 *Our Mission*, Nat'l Sec. Agency/Cent. Sec. Serv., https://www.nsa.gov/ (visited July 1, 2024).

52 Press Release, Nat'l Sec. Agency, General Nakasone Offers Insight into Future of Cybersecurity and SIGINT (Sep. 21, 2023), https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3533425/gen-nakasone-offers-insight-into-future-of-cybersecurity-and-sigint/.

53 Press Release, Nat'l Sec. Agency, Artificial Intelligence: Next Frontier is Cybersecurity (July 23, 2021), https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2702241/artificial-intelligence-next-frontier-is-cybersecurity/; Jay Stanley, *Will ChatGPT Revolutionize Surveillance?*, ACLU (Apr. 19, 2023), https://www.aclu.org/news/privacy-technology/will-chatgpt-revolutionize-surveillance; *An Interview with Paul M. Nakasone*, 92 Joint Force Q., 4 (Jan. 2019), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-

Interview.pdf; Justin Doubleday, *NSA Working on New AI 'Roadmap' as Intel Agencies Grapple with Recent Advances*, Fed. News Network (July 14, 2023), https://federalnewsnetwork.com/artificial-intelligence/2023/07/nsa-working-on-new-ai-roadmap-as-intel-agencies-grapple-with-recent-advances/; Matt Kapko, *3 Areas of Generative AI the NSA Is Watching in Cybersecurity*, Cybersecurity Dive (May 1, 2023), https://www.cybersecuritydive.com/news/nsa-watching-generative-ai/649041/; Carolyn Shapiro, *The Intelligence Community Is Developing New Uses for AI*, FedTech (Oct. 4, 2022), https://fedtechmagazine.com/article/2022/10/intelligence-community-developing-new-uses-ai-perfcon.

54 National Security Commission on Artificial Intelligence, The Final Report, 108–18.

55 *See, e.g.,* Faiza Patel, Elizabeth Goitein & Amos Toh, Brennan Ctr. for Justice, Overseas Surveillance in an Interconnected World, (Mar. 16, 2016), https://www.brennancenter.org/our-work/research-reports/overseas-surveillance-interconnected-world; Dustin Volz, *FBI Conducted Potentially Millions of Searches of Americans' Data Last Year, Report Says*, Wall Street J. (Apr. 29, 2022), https://www.wsj.com/articles/fbi-conducted-potentially-millions-of-searches-of-americans-data-last-year-report-says-11651253728.

56 *Artificial Use Case Inventory—Customs and Border Protection: Port of Entry Risk Assessments*, Dep't Homeland Sec., https://www.dhs.gov/data/AI_inventory (last visited Aug. 26, 2024). In 2021, CBP stated that it used "predictive analytics," a type of analysis typically based on machine learning, as part of ATS's UPAX module, which generates risk assessments of travelers. *See* Dep't Homeland Sec., 2020 & 2021 Data Mining Rep. 16 (Aug. 2022), https://www.dhs.gov/sites/default/files/2023-08/23_0831_priv_dhs-data-mining-report.pdf.

57 *Artificial Use Case Inventory—Customs and Border Protection: Port of Entry Risk Assessments,* Dep't Homeland Sec., https://www.dhs.gov/data/AI_inventory (last visited Aug. 26, 2024); Dep't Homeland Sec., Priv. Impact Assessment Update for the Automated Targeting Sys. DHS/CBP/PIA-006(e) 1, 2-3, 21-22, 26 (Jan. 13, 2017), https://www.dhs.gov/sites/default/files/2022-07/privacy-pia-cbp006-ats-july2022_0.pdf [hereinafter Data Mining Rep.].

58 Data Mining Rep. at 26; Gov. Accountability Off., No. GOA-17-216, Border Security: CBP Aims to Prevent High-Risk Travelers from Boarding U.S.-Bound Flights, But Needs to Evaluate Program Performance 10 (Jan. 2017), https://www.gao.gov/assets/gao-17-216.pdf [hereinafter CBP GAO Report] ("CBP identifies unknown high-risk individuals by comparing their information against a set of targeting rules based on intelligence, law enforcement, and other information.").

59 Memorandum from Joseph V. Cuffari, Inspector Gen., to David Pekoske, Administrator Transp. Sec. Admin. 1 n.2 (Nov. 25, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-11/OIG-21-11-Nov20-Redacted.pdf.

60 Letter from the ACLU to the House Energy & Com. Comm. (July 18, 2022), https://www.aclu.org/documents/aclu-statement-american-data-privacy-protection-act-ahead-committee-markup.

61 Letter from the ACLU to the House Energy and Com. Comm. (June 25, 2024), https://www.aclu.org/documents/aclu-coalition-call-for-restoration-of-crucial-civil-rights-protections-in-federal-privacy-bill.

62 Letter from the ACLU to the House Subcomm. on Innovation, Data & Com. (June 17, 2024), https://www.aclu.org/documents/aclu-affiliates-lead-coalition-letter-with-local-state-and-national-advocacy-organizations-raising-concerns-about-apras-approach-to-preemption.