EXHIBIT F

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF KENTUCKY

UNITED STATES OF AMERICA, Plaintiff, v. MICHAEL ADAMS, in his official capacity as Kentucky Secretary of State, *et al.* Defendants.	No. 3:26-cv-00019-GFVT

MOTION TO DISMISS OF INTERVENOR-DEFENDANTS
THE LEAGUE OF WOMEN VOTERS OF KENTUCKY,
THE NEW AMERICANS INITIATIVE, ZITSI MIRAKHUR, AND JOERN SOLTAU

TABLE OF CONTENTS

INTRODUCTION

In this action—one of dozens filed across the country—the United States seeks to compel the disclosure of voters' sensitive personal data to which it is not entitled, using civil rights laws as a pretext. This effort fails as a matter of law: the Complaint does not plausibly allege that the United States has provided the statutorily required basis and purpose for its request, or that production of sensitive voter information is necessary.

Congress has repeatedly legislated to protect the franchise, including through Title III of the Civil Rights Act of 1960 ("CRA" or "Title III"), 52 U.S.C. § 20701 *et seq*., as well as the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 *et seq*., and the Help America Vote Act ("HAVA"), 52 U.S.C. § 20901 *et seq*. The purpose of these statutes is to ensure that all eligible Americans—especially racial minorities and voters with disabilities—can participate in free, fair, and secure elections. As DOJ itself has explained, Title III of the CRA, the election records provision invoked in the Complaint here, was designed to "secure a more effective protection of the right to vote." U.S. Dep't of Just., Civ. Rts. Div., *Federal Law Constraints on Post-Election "Audits"* (Jul. 28, 2021), https://perma.cc/74CP-58EH (citing *State of Ala. ex rel. Gallion v. Rogers*, 187 F. Supp. 848, 853 (M.D. Ala. 1960), and H.R. Rep. No. 86-956 (1959)).

The federal government's demand for Kentucky's unredacted voter file—which contains sensitive personal information including driver's license and Social Security numbers from millions of Kentuckians—violates the CRA and undermines its core purpose of protecting voting access. Releasing unredacted voter records for purposes unrelated to voter access would deter voter participation and undermine the right to vote. This is especially true here: the government's actual purpose—widely reported but never disclosed in its request—is to build an unauthorized and unlawful national voter database to illegally target and challenge voters.

The Complaint does not adequately plead that the United States has met the requirements of the CRA, which mandates the government fully and accurately set forth "the basis and the purpose" for its data request, 52 U.S.C. § 20703. District courts in California and Oregon recently reached this exact conclusion with respect to materially identical complaints seeking those states' complete voter files, dismissing the United States' claims without leave to replead. *See United States v. Weber*, No. 2:25-CV-9149-DOC-ADS, 2026 WL 118807 (C.D. Cal. Jan. 15, 2026); *United States v. Oregon*, No. 6:25-cv-1666-MTK, 2026 WL 318402 (D. Or. Feb. 5, 2026); *see also* Op., *United States v. Benson*, No. 1:25-cv-1148-HYJ-PJG (W.D. Mich. Feb. 10, 2026), Dkt. No. 67 (dismissing CRA claims on other grounds). This Court should do the same.

BACKGROUND

I. The United States seeks to force the disclosure of voters' sensitive voter data.

Beginning in May 2025, the DOJ began sending letters to election officials in at least forty states, making escalating demands for the production of voter registration databases, with plans to gather data from all fifty states. *See* Kaylie Martinez-Ochoa, Eileen O'Connor, & Patrick Berry, Tracker of Justice Department Requests for Voter Information, Brennan Ctr. for Just. (updated Mar. 4, 2026), https://perma.cc/M6QS-THRS.

DOJ has allegedly sent Defendants letters on July 17, August 8, and August 14, 2025, demanding, among other things, an electronic copy of Kentucky's statewide voter registration list that includes "all fields" it claims are "required under Section 303 of HAVA." Compl. ¶¶ 20–25. Per the August 14 letter—according to the Complaint—DOJ has explained that its request for "all fields" must include voters' full name, date of birth, residential address, driver's license number,

and the last four digits of the registrant's Social Security number. Compl. ¶ 24. DOJ has claimed that it needs this list for purposes of enforcing the NVRA and HAVA. Compl. ¶¶ 20–25, 29.

According to the Complaint, "Defendants refused the Attorney General's demand" on August 22, 2025. *Id.* ¶ 26. DOJ then sent Defendants an email with a "proposed memorandum of understanding ('MOU')" it claimed "'satisfies all reasonable concerns regarding privacy and data security.'" *Id.* ¶¶ 28–30 (citing December 2, 2025 Email). The Complaint claims Defendants took no action on the MOU and, as of the date of the Complaint, "have refused to comply with the Attorney General's demand." *Id.* ¶¶ 31–33.

In response, the United States brought this lawsuit, one of at least thirty similar suits against states across the country.[1]

II. The United States seeks to unlawfully construct a national voter database with the data.

As documented in public reporting, DOJ's requests for sensitive voter data from Kentucky and other states appear to be part of a broader effort to construct a national voter database—using

[1] *See* Press Release, U.S. Dep't of Just., *Justice Department Sues Five Additional States for Failure to Produce Voter Rolls* (Feb. 26, 2026), https://perma.cc/67UZ-KJFY; Press Release, U.S. Dep't of Just., *Justice Department Sues Virginia for Failure to Produce Voter Rolls* (Jan. 16, 2026), https://perma.cc/3L8Q-SJM5; Press Release, U.S. Dep't of Just., *Justice Department Sues Arizona and Connecticut for Failure to Produce Voter Rolls* (Jan. 6, 2026), https://perma.cc/6QP2-8ZXC; Press Release, U.S. Dep't of Just., *Justice Department Sues Four States for Failure to Produce Voter Rolls* (Dec. 18, 2025), https://perma.cc/HHJ7-JWQQ; Press Release, U.S. Dep't of Just., *Justice Department Sues Four Additional States and One Locality for Failure to Comply with Federal Elections Laws* (Dec. 12, 2025), https://perma.cc/TQ5T-FB2A; Press Release, U.S. Dep't of Just., *Justice Department Sues Six Additional States for Failure to Provide Voter Registration Rolls* (Dec. 2, 2025), https://perma.cc/F5MD-NWHD; Press Release, U.S. Dep't of Just., *Justice Department Sues Six States for Failure to Provide Voter Registration Rolls* (Sept. 25, 2025), https://perma.cc/7J99-WGBA; Press Release, U.S. Dep't of Just., *Justice Department Sues Oregon and Maine for Failure to Provide Voter Registration Rolls* (Sept. 16, 2025), https://perma.cc/M69P-YCVC. The United States' first suit seeking Georgia's voter registration file was dismissed because of improper venue. *See United States v. Raffensperger*, No. 5:25-cv-548-CAR, 2026 WL 184233 (M.D. Ga. Jan. 23, 2026).

untested database matching techniques to scrutinize state voter rolls and, in effect, to "nationalize" elections.

According to this reporting, federal employees "have been clear that they are interested in a central, federal database of voter information." Devlin Barrett & Nick Corasaniti, *Trump Administration Quietly Seeks to Build National Voter Roll*, N.Y. TIMES, Sept. 9, 2025, https://www.nytimes.com/2025/09/09/us/politics/trump-voter-registration-data.html. DOJ is coordinating these novel efforts with the federal Department of Homeland Security ("DHS"), according to reported statements from DOJ and DHS. *Id.*[2] One article extensively quoted a lawyer who recently left DOJ's Civil Rights Division, describing the Administration's aims in these cases:

> We were tasked with obtaining states' voter rolls, by suing them if necessary. Leadership said they had a DOGE person who could go through all the data and compare it to the Department of Homeland Security data and Social Security data . . . I had never before told an opposing party, Hey, I want this information and I'm saying I want it for this reason, but I actually know it's going to be used for these other reasons. That was dishonest. It felt like a perversion of the role of the Civil Rights Division.

Emily Bazelon & Rachel Poser, *The Unraveling of the Justice Department*, N.Y. TIMES MAG., Nov. 16, 2025, https://www.nytimes.com/interactive/2025/11/16/magazine/trump-justice-department-staff-attorneys.html.

Indeed, publicly-disclosed documents have confirmed that DOJ has asked staffers from the new "Department of Governmental Efficiency" ("DOGE") to identify noncitizens in state voter

[2] *See also, e.g.*, Jonathan Shorman, *DOJ is Sharing State Voter Roll Lists with Homeland Security*, STATELINE, Sept. 12, 2025, https://stateline.org/2025/09/12/doj-is-sharing-state-voter-roll-lists-with-homeland-security; Sarah Lynch, *US Justice Dept Considers Handing over Voter Roll Data for Criminal Probes, Documents Show*, REUTERS, Sept. 9, 2025, https://www.reuters.com/legal/government/us-justice-dept-considers-handing-over-voter-roll-data-criminal-probes-documents-2025-09-09.

rolls by matching voter data with data from the Social Security Administration.[3] DOJ officials have since claimed that "we've checked 47.5 million voting records" and found "several thousand non-citizens who are enrolled to vote in Federal elections," although reporting indicates that these efforts are producing false positives—*i.e.*, that they are flagging U.S. citizens as being non-citizens who are ineligible to vote.[4]

According to additional public reporting, these efforts are being conducted with the involvement of self-proclaimed election integrity advocates within and outside the government who have previously sought to disenfranchise voters and overturn elections. Those advocates include Heather Honey, who sought to overturn the result of the 2020 presidential election in multiple states and now serves as DHS's "deputy assistant secretary for election integrity."[5] Also involved is Cleta Mitchell, a private attorney and leader of a national group called the "Election Integrity Network," who has, among other things, promoted the use of artificial intelligence to challenge registered voters.[6]

---

[3] *E.g.*, Miles Parks & Jude Joffe-Block, *Trump's DOJ focuses in on voter fraud, with a murky assist from DOGE*, NPR (May 22, 2025), https://perma.cc/X3Q6-AFJU .

[4] December 5, 2025 Post by @AAGDhillon, https://x.com/AAGDhillon/status/1997003629442519114; Jude Joffe-Block, *Trump's SAVE Tool Is Looking for Noncitizen Voters. But It's Flagging U.S. Citizens Too*, NPR (Dec. 10, 2025), https://perma.cc/6PY2-3F3D .

[5] *See* Alexandra Berzon & Nick Corasaniti, *Trump Empowers Election Deniers, Still Fixated on 2020 Grievances*, N.Y. TIMES, Oct. 22, 2025, https://www.nytimes.com/2025/10/22/us/politics/trump-election-deniers-voting-security.html (documenting "ascent" of election denier Honey); Jen Fifield, *Pa.'s Heather Honey, Who Questioned the 2020 Election, Is Appointed to Federal Election Post*, PA. CAPITAL-STAR, Aug. 27, 2025, https://penncapital-star.com/election-2025/pa-s-heather-honey-who-questioned-the-2020-election-is-appointed-to-federal-election-post; Doug Bock Clark, *She Pushed to Overturn Trump's Loss in the 2020 Election. Now She'll Help Oversee U.S. Election Security*, PROPUBLICA, Aug. 26, 2025, https://perma.cc/CE7A-6RY6.

[6] *See, e.g.*, Matt Cohen, *DHS Said to Brief Cleta Mitchell's Group on Citizenship Checks for Voting*, DEMOCRACY DOCKET, June 12, 2025, https://www.democracydocket.com/news-alerts/dhs-said-to-brief-cleta-mitchells-anti-voting-group-on-checking-citizenship-for-voters; *see also* Jude Joffe-Block & Miles Parks, *The Trump Administration Is Building a National Citizenship Data System*,

A recent federal court filing by DOJ corroborates how United States officials have been seeking to use voter data in conjunction with data-matching and aggregation techniques, with these outside "election integrity" advocates. As detailed in the filing, which was made on behalf of the U.S. Social Security Administration (SSA):

> SSA determined in its recent review that in March 2025, a political advocacy group contacted two members of SSA's DOGE Team with a request to analyze state voter rolls that the advocacy group had acquired. The advocacy group's stated aim was to find evidence of voter fraud and to overturn election results in certain States. In connection with these communications, one of the DOGE team members signed a "Voter Data Agreement," in his capacity as an SSA employee, with the advocacy group. He sent the executed agreement to the advocacy group on March 24, 2025.

Notice of Corrections to the Record at 5, *Am. Fed'n of State, Cnty. & Mun. Emps. v. Soc. Sec. Admin.*, No. 25-cv-596, Dkt. No. 197 (D. Md. Jan. 16, 2026); *see also* Kyle Cheney, *Trump Administration Concedes DOGE Team May Have Misused Social Security Data*, POLITICO, Jan. 20, 2026, https://www.politico.com/news/2026/01/20/trump-musk-doge-social-security-00737245. The filings, which do not specify the terms of the "Voter Data Agreement" or the activities these DOGE actors or others undertook pursuant to it, also indicated that, around the same period, DOGE actors also shared unknown amounts of social security data on an unapproved third-party server, in a "manner [that] is outside SSA's security protocols." Notice of Corrections to the Record, *supra*, at 6.

The current administration has made clear these efforts' purpose. Last month, President Trump announced his desire to "nationalize" elections in certain states: "The Republicans should

---

NPR, June 29, 2025, https://perma.cc/J8VZ-X4N4 (reporting that Mitchell had received a "full briefing" from federal officials); *see also* Andy Kroll & Nick Surgey, *Inside Ziklag, the Secret Organization of Wealthy Christians Trying to Sway the Election and Change the Country*, PROPUBLICA, July 13, 2024, https://perma.cc/5W2N-SS2Q ("Mitchell is promoting a tool called EagleAI, which has claimed to use artificial intelligence to automate and speed up the process of challenging ineligible voters.").

say, 'We want to take over,'" he said. "We should take over the voting, the voting in at least many—15 places. The Republicans ought to nationalize the voting." Reid Epstein & Nick Corasaniti, *Trump, in an Escalation, Calls for Republicans to 'Nationalize' Elections*, N.Y. TIMES, Feb. 2, 2026, https://www.nytimes.com/2026/02/02/us/politics/trump-nationalize-elections.html.

III. The United States seeks to unlawfully use the data to disenfranchise voters.

Additional federal government documents reveal how that the United States plans to use voters' sensitive personal data: to assert control over voting eligibility, "nationalize" elections, order voter disenfranchisement, and potentially contest election results. In connection with its requests for states' voter data, the United States has begun asking states to execute a memorandum of understanding describing the data's intended use. *See* Ex. 1, U.S. Dep't of Just., Civ. Div., Confidential Mem. of Understanding ("MOU").[7] The MOU purports to grant the United States broad new authority to identify allegedly ineligible voters on state rolls and then compel their removal, depriving them of the franchise.

The NVRA and HAVA require states to make a "reasonable effort" to maintain voter lists and remove ineligible voters. 52 U.S.C. § 20507(a)(4); § 21083(a)(4)(A). The specific procedures for complying with HAVA's centralized voter file requirement are "left to the discretion of the State." 52 U.S.C. § 21085. The NVRA also protects voters by requiring that certain potentially ineligible voters remain on the rolls for two election cycles before removal, reducing the risk of erroneously purging ineligible voters. *Id.* § 20507(d)(1)(B). That reflects Congress's core goals

[7] This Court may take judicial notice of the MOU as a DOJ-produced judicial document. *See Yoder v. Bowen*, 146 F.4th 516, 526 n.1 (6th Cir. 2025) (citing Fed. R. Evid. 201(b); relevant cases); *Colston v. Boston Mkt. Corp.*, No. 2:17-cv-11649, 2018 WL 1404417, at *4 (E.D. Mich. Feb. 14, 2018) ("[T]he Court may take judicial notice of a fact that 'can be accurately readily determined from sources whose accuracy cannot be reasonably questioned . . . .'" (quoting Fed. R. Evid. 201(b)(2)).

with the NVRA: protecting and expanding the right to register to vote and participate in democracy. *E.g.*, 52 U.S.C. § 20501.

The MOU's terms, however, purport to vest authority to identify ineligible voters in the federal government. MOU at 2, 5. It designates DOJ a "Custodian" of the state's voter file and requires DOJ to analyze that file and identify "any voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns," bearing on whether the list "only includes eligible voters." MOU at 5. Once federal officials flag voters as ineligible, states would be required to remove them "within forty-five (45) days" and resubmit their voter lists for further review. *Id.* These removals would be required regardless of the NVRA's procedural protections—including its firm prohibition on systematic voter removals within 90 days of an election, 52 U.S.C. § 20507.[8]

In short, extensive public reporting, court filings, and DOJ officials' statements and admissions indicate that the United States's aim in seeking sensitive voter data is to turn states' voter rolls into a tool to unlawfully and improperly mass-challenge voters and interfere with states' democratic processes.

Recent events further underscore the anomalous nature of the United States' request. On January 24, 2026, Attorney General Pamela Bondi wrote a letter to Minnesota Governor Tim Walz, regarding DHS's "Operation Metro Surge" in the Twin Cities.[9] Like Kentucky, Minnesota has been

---

[8] *See also* Jonathan Shorman, *Trump's DOJ Offers States 'Confidential' Deal to Wipe Voters Flagged by Feds as Ineligible*, STATELINE, Dec. 18, 2025, https://stateline.org/2025/12/18/trumps-doj-offers-states-confidential-deal-to-wipe-voters-flagged-by-feds-as-ineligible/.

[9] *Read Bondi's Letter to Minnesota's Governor*, N.Y. TIMES (Jan. 24, 2026), https://www.nytimes.com/interactive/2026/01/24/us/pam-bondi-walz-doc.html ("Bondi Letter"); *see also* Order, *Tincher v. Noem*, No. 25 Civ. 4669 (D. Minn. Jan. 16, 2026), Dkt. No. 85 (granting injunction against certain DHS practices towards the civilian population of Minneapolis-St. Paul in connection with purported immigration enforcement operations there).

sued by the federal government for access to its unredacted voter rolls. The letter lists three actions Minnesota must take to "restore the rule of law, support ICE officers, and bring an end to the chaos"—one being to "allow the Civil Rights Division of the Department of Justice to access voter rolls to confirm that Minnesota's voter registration practices comply with federal law as authorized by the Civil Rights Act of 1960."[10]

LEGAL STANDARD

A court must dismiss a complaint that fails to "state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). The court accepts well-pleaded factual allegations as true but need not accept legal conclusions or "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements." *Ashcroft v. Iqbal*, 556 U.S. 662, 678–79 (2009). A complaint must "'nudge[] the[] claim[] across the line from conceivable to plausible," or face dismissal. *Kovalchuk v. City of Decherd*, 95 F.4th 1035, 1037 (6th Cir. 2024) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). In assessing a complaint, courts may consider documents incorporated by reference and matters subject to judicial notice. *Solo v. United Parcel Serv. Co.*, 819 F.3d 788, 794 (6th Cir. 2016).

ARGUMENT

Against the backdrop of the turmoil of the Jim Crow era, Congress enacted the CRA, including the public records provisions in Title III, to facilitate investigations of civil rights violations preventing eligible citizens from voting due to discrimination. H.R. Rep. No. 86-956 at 7 (1959) (indicating the purpose of Title III "is to provide a more effective protection of the right of all qualified citizens to vote without discrimination on account of race"). But the Attorney

[10] Bondi Letter at 2–3.

General's access to these records is not unbounded. If the Attorney General makes a demand for records, she must provide "a statement of the basis and the purpose therefor." 52 U.S.C. § 20703.

The Complaint fails to adequately plead a claim for relief under the CRA for at least two distinct reasons. *First*, the United States fails to plausibly establish that it has offered the required statement of "the basis and the purpose" of its sweeping demand for Kentucky's full and unredacted state voter registration list, giving insufficient and pretextual explanations. *Second*, the United States does not make any showing that turning over *unredacted* records, replete with private voter information, is required under the CRA. Instead, producing this data would run directly contrary to the CRA, which exists to protect the right to vote. The privacy and constitutional rights of Kentucky voters are paramount and invoking the CRA to invade those rights is a distortion of what the CRA was created to do.

I. The United States' demand fails to meet the CRA's requirements.

Title III of the CRA sets out retention requirements regarding federal election records: Section 301 requires officers of elections to "retain and preserve, for a period of twenty-two months from the date of any" federal election, "all records and papers which come into [their] possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election," with certain exceptions regarding delivery and designation of custodians. 52 U.S.C. § 20701. Section 303 requires that "[a]ny record or paper" retained and preserved under Section 301 "shall, upon demand in writing by the Attorney General or [her] representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or [her] representative." *Id*. § 20703. "This demand shall contain a statement of *the basis and the purpose therefor*." *Id*. (emphasis added).

Contemporaneous case law immediately following Title III's enactment shows that the required "basis" and "purpose" were distinct concepts. *Kennedy v. Lynd*, 306 F.2d 222, 229 n.6 (5th Cir. 1962); *In re Coleman*, 208 F. Supp. 199, 199–200 (S.D. Miss. 1962), *aff'd sub nom*., *Coleman v. Kennedy*, 313 F.2d 867 (5th Cir. 1963). The "basis" is an explanation of why the Attorney General believes a federal civil rights violation has occurred—specifically, "a factual basis for investigating a violation of a federal statute," *Lynd*, 306 F.2d at 229 n.6, supported by "specific, articulable facts," *Weber*, 2026 WL 118807, at *9. The "purpose" is an explanation of how the requested records would help determine whether such a violation exists and must "relate to a purpose of investigating violations of individuals' voting rights." *Oregon*, 2026 WL 318402, at *11; *see also Lynd*, 306 F.2d at 229 n.6.

The Complaint fails to provide "a statement of the basis and the purpose" needed to support disclosure of the unredacted voter file. 52 U.S.C. § 20703. It offers only the conclusory allegation: "The written demand 'contain[ed] a statement of the basis and the purpose therefor.'" Compl. ¶ 36 (citation omitted). But the Complaint does not supply a "basis" for believing Kentucky's list maintenance procedures violate the NVRA or HAVA—no evidence of anomalies, no suggestion that anything is amiss. *Id.* ¶¶ 23–25. Rather than "specific, articulable facts pointing to the violation of federal law," *Weber*, 2026 WL 118807, at *9, these documents offer only the legal conclusion that the CRA's requirements were satisfied. That is not enough to survive a motion to dismiss.

Even if the United States had provided a proper "basis" for its demand—and it did not—it fails to explain any connection between its purported "purpose" and the request for the full and unredacted voter file. The Complaint does not explain why unredacted voter files are necessary to determine whether Kentucky has "conduct[ed] a general program that makes a reasonable effort to remove the names of ineligible voters" by virtue of "death" or "a change in the residence of the

registrant." Compl. ¶ 12 (citing 52 U.S.C. § 20507). The NVRA and HAVA both leave the mechanisms for conducting list maintenance within a state's discretion. *See* 52 U.S.C. § 20507(a)(4), (c)(1); *id.* § 21083(a)(2)(A); *id.* § 21085. The procedures carried out by a state or locality establish their compliance; the unredacted voter file does not. Even if the United States identified voters who had moved or died on Kentucky's voter list at a single point in time, that would not amount to Kentucky failing to comply with the "reasonable effort" required by the NVRA or HAVA. *See, e.g.*, *Pub. Int. L. Found. v. Benson*, 136 F.4th 613, 624–27 (6th Cir. 2025) (describing a "reasonable effort" as "a serious attempt that is rational and sensible").

The basis and purpose requirement is a "critical safeguard that ensures the request is legitimately related to the purpose of the statute." *Weber*, 2026 WL 118807, at *9. It is not perfunctory—it demands a specific statement of why the information is sought and how it will aid the investigation. *See Oregon*, 2026 WL 318402, at *9 ("If *any* purpose—regardless of its relationship to the purposes of the statute itself—would suffice, then the requirement of stating the demand's purpose would serve no function."). Courts applying analogous requirements to administrative subpoenas have held that enforcement is proper only where the investigation serves "a legitimate purpose," *United States v. Powell*, 379 U.S. 48, 57 (1964), and that subpoenas issued in "bad faith," ought not to be enforced. *United States v. Markwood*, 48 F.3d 969, 978 (6th Cir. 1995). Such requirements ensure that the information sought is relevant and not unduly burdensome. *See, e.g.*, *Doe v. United States*, 253 F.3d 256, 263 (6th Cir. 2001) (reciting requirements for investigation via administrative subpoena). The CRA's basis and purpose requirement serves the same function: preventing the statute from being weaponized as a "fishing expedition" to obtain records for speculative, impermissible, or legally unauthorized reasons

unrelated to the CRA's aims. *Weber*, 2026 WL 118807, at *9; *see also Blue Cross, Blue Shield of Ohio v. Klein*, No. 96-3805, 1997 WL 400095, at *3 (6th Cir. 1997) (unpublished).

As such, even if some voting records were necessary to investigate Kentucky's NVRA list maintenance compliance, the United States has not justified demanding the *full* unredacted voter file. For decades, DOJ has neither sought nor required a full, unredacted voter file in NVRA compliance investigations. *See, e.g.*, Press Release, U.S. Dep't of Just., *United States Announces Settlement with Kentucky Ensuring Compliance with Voter Registration List Maintenance Requirements* (July 5, 2018) https://perma.cc/G2EZUUA5 (describing letters to all 44 states covered by the NVRA with requests for list maintenance information, but without demanding voter files). The United States' failure to articulate the basis and the purpose for its demand is fatal to its request.

The government's statement is not just legally insufficient—it is also pretextual. Section 303 requires "the basis and the purpose" of a records request, and by twice using the definite article, the statute demands the *actual* basis and purpose underlying the request, not just "*a*" basis or purpose among many. *See Niz-Chavez v. Garland*, 593 U.S. 155, 165–66 (2021); *see also, e.g.*, *Corner Post, Inc. v. Bd. of Governors of the Fed. Rsrv. Sys.*, 603 U.S. 799, 817 (2024) (emphasizing distinction between the definite and indefinite article). But the United States has not disclosed its actual purpose, and this Court "is not obliged to accept a contrived statement and purpose" in its place. *Weber*, 2026 WL 118807, at *10.

Such a database would be unlawful on multiple grounds. Congress has never authorized a national voter database—let alone one designed to target and mass-challenge voters. Its creation alone would violate, among other provisions, the Privacy Act's prohibition on maintaining any

database "describing how any individual exercises rights guaranteed by the First Amendment," which necessarily includes the right to vote. *See* 5 U.S.C. § 552a(e)(7).

Consider also the MOU that the United States has recently pushed several states to sign in connection with its requests for statewide voter files. *See* Compl. ¶¶ 28–30; MOU at 7–8. The NVRA and HAVA require states—not the federal government—to make "reasonable effort" to remove ineligible voters, 52 U.S.C. §§ 20507(a)(4), 21083(a)(4)(A), with methods of compliance "left to the discretion of the State," *id.* § 21085. The proposed MOU would violate these requirements in at least two ways. First, it purports to vest authority to identify ineligible voters in the hands of the federal government, contrary to the statute. MOU at 2, 5. Second, it would compel states to remove flagged voters "within forty-five (45) days," *id.* at 5—in violation of the NVRA's procedural protections for voters. 52 U.S.C. § 20507.

Finally, there is the Attorney General's recent letter to Minnesota Governor Tim Walz, demanding that Minnesota turn over voters' private data to help "support ICE officers" and "bring an end to the chaos" being inflicted on the civilian population there by DHS agents. *See* Bondi Letter at 2–3. By explicitly linking DOJ's request for voter data to the Administration's immigration enforcement efforts, the letter further exposes DOJ's failure to disclose the true purpose of its demands. Indeed, the federal court in *Oregon* reached the same conclusion: the context of a voter data demand within a letter about immigration enforcement "casts serious doubt as to the true purposes for which Plaintiff is seeking voter registration lists in this and other cases, and what it intends to do with that data." 2026 WL 318402, at *11.

The United States' failure to honestly disclose what it is doing—and will do—with voters' sensitive personal information is independently fatal to the CRA claim. Because the government has not stated its true purpose for demanding Kentuckians' protected personal data, it cannot

invoke the NVRA, Civil Rights Act, or HAVA as cover. Those statutes were passed to "protect voting rights," not to provide "DOJ . . . the guise of a pretextual investigative purpose." *Weber*, 2026 WL 118807, at *12. Accordingly, courts have recently observed that the presumption that the government "could be taken at its word" in this context, "with little doubt about its intentions and stated purposes—no longer holds." *Oregon*, 2026 WL 318402, at *11.

II. The United States seeks records outside the scope of Title III.

On the requests' merits, the Western District of Michigan very recently held that the United States' request for a statewide voter file sought records is not covered by Title III. *See Benson*, 2026 WL 362789, at *11. The same is true here.

Section 301 requires elections officials to "retain and preserve, for a period of twenty-two months from the date of any" federal election, "all records and papers which come into [their] possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election." 52 U.S.C. § 20701. Section 303—which grants the Attorney General authority to request records—obligates officials to produce only those records Section 301 requires them to retain, i.e., records that have "come into [their] possession." *Id.* § 20701. While "all records and papers" is sweeping language, Title III is distinct from other records statutes in that its text limits itself. Indeed, as *Benson* held, "come into . . . possession," refers to records that elections officials *obtain*, not those they *create*. 2026 WL 362789, at *9 ("Congress frequently uses the phrase 'come into possession' to refer to items that a person *obtains* rather than *creates*." (compiling statutes)). Other courts in this Circuit and the Supreme Court have similarly equated "coming into possession" with receipt. *See, e.g.*, *Honeycutt v. United States*, 581 U.S. 443, 449 (2017) (defining "obtain" as "to come into possession of" (quoting Random House Dictionary of the English Language 995 (1966))); *Nat'l Sign & Signal v. Livingston*, 422 B.R. 645, 650 (W.D.

Mich. 2009) ("'Obtain' means 'to come into possession of; get, acquire." (quoting Webster's New Universal Unabridged Dictionary 1139 (2003))); *cf. also Sekhar v. United States*, 570 U.S. 729, 734 (2013) ("Obtaining property requires '. . . the acquisition of property.'" (citation omitted)).

What was true to Michigan in *Benson* is true here: Kentucky's statewide voter registration file is a live, continuously updated document created by state officials—not a record or paper "which come[s] into [election officials'] possession." 52 U.S.C. § 20701; *Benson*, 2026 WL 362789, at *10. The records DOJ seeks are ones Kentucky officials *create*, not ones that "come into [their] possession." 52 U.S.C. § 20701. DOJ's request therefore falls outside Title III and fails as a matter of law.

III. Any records disclosed under the CRA should be redacted to protect the constitutional rights of the voter, so the Court must deny the United States' request.

Even if disclosure were appropriate, sensitive personal voter information would still be subject to redaction. Indeed, courts have found that redaction may be required to prevent the disclosure of sensitive personal information that would create an intolerable burden on the constitutional right to vote. The cases interpreting Section 8(i) of the NVRA are instructive, as courts have consistently permitted—and sometimes required—redaction of voters' sensitive personal data before disclosure to protect voter privacy and ensure compliance with federal and state law and the Constitution.

Like the CRA, the NVRA is silent as to how sensitive personal information should be treated during disclosure. *See* 52 U.S.C. § 20703; § 20507(i)(1). Under the doctrine of constitutional avoidance, courts must interpret the disclosure provisions in a manner that does not unconstitutionally burden the right to vote. *See Torres v. Precision Indus., Inc.*, 938 F.3d 752, 754 (6th Cir. 2019). Federal courts have consistently struck this balance, interpreting the "all records concerning" language in Section 8(i) to permit—and sometimes require—redaction of confidential

materials. As the First Circuit has noted, "nothing in the text of the NVRA prohibits the appropriate redaction of uniquely or highly sensitive personal information in the Voter File," and such redaction "can further assuage the potential privacy risks implicated by the public release of the Voter File." *Pub. Int. L. Found., Inc. v. Bellows*, 92 F.4th 36, 56 (1st Cir. 2024).[11]

Redaction also may be affirmatively required if disclosure would "create[] an intolerable burden on [the constitutional right to vote] as protected by the First and Fourteenth Amendments." *Project Vote/Voting for Am. v. Long*, 682 F.3d 331, 339 (4th Cir. 2012). In *Long*, the Fourth Circuit, even while granting access to voter registration applications, affirmed the importance of redacting Social Security numbers as "uniquely sensitive and vulnerable to abuse," emphasizing that unredacted release risked deterring citizens from registering and thus imposed an "intolerable burden" on this fundamental right. *Id*. at 334, 339; *cf. In re Coleman*, 208 F. Supp. at 200 (noting, in the context of a Title III records request, multiple considerations which could be "[s]ignificant," including whether "official records are privileged, or exempt from discovery for any sound reason of public policy," or "that an inspection of these records would be oppressive, or any unlawful invasion of any personal constitutional right"). As such, public disclosure provisions such as those in the NVRA and Title III must therefore be interpreted to avoid this unconstitutional burden. *See Long*, 682 F.3d at 339; *Bellows*, 92 F.4th at 56. That danger is present here. *See, e.g.*, Mot. to Intervene, Ex. B, Decl. of Jennifer Jackson, M.D. ¶¶ 8, 10; Mot. to Intervene, Ex. C, Decl. of

[11] *See also Pub. Int. L. Found., Inc. v. N.C. State Bd. of Elections*, 996 F.3d 257, 264 (4th Cir. 2021) (NVRA disclosure provisions "must be read in conjunction with the various statutes enacted by Congress to protect the privacy of individuals and confidential information held by certain governmental agencies" and protecting sensitive information from disclosure); *Pub. Int. L. Found., Inc. v. Dahlstrom*, 673 F. Supp. 3d 1004, 1015–16 (D. Alaska 2023) (similar); *Pub. Int. L. Found., Inc. v. Matthews*, 589 F. Supp. 3d 932, 942 (C.D. Ill. 2022), *clarified on denial of reconsideration*, No. 20-CV-3190, 2022 WL 1174099 (C.D. Ill. Apr. 20, 2022) (similar).

Nirupama Kulkarni ¶¶ 8–10; Mot. to Intervene, Ex. D, Decl. of Zitsi Mirakhur ¶¶ 13–14; Mot. to Intervene, Ex. E., Decl. of Joern Soltau ¶ 12.

The same privacy and constitutional concerns that warrant redactions under the NVRA apply equally to requests under the CRA. *Cf. Sheetz v. Cnty. of El Dorado*, 601 U.S. 267, 281–82 (2024) (Gorsuch, J., concurring) ("[O]ur Constitution deals in substance, not form. However the government chooses to act, . . . it must follow the same constitutional rules."). And the limited case law considering CRA records requests acknowledges that courts retain the "power and duty to issue protective orders," *Lynd*, 306 F.2d at 230, such as requiring redaction of sensitive fields that courts have consistently determined are entitled to protection from disclosure.

CONCLUSION

For all of these reasons, Proposed Intervenor-Defendants respectfully request that the United States' Complaint be dismissed.

Dated: March 6, 2026
/s/ Corey M. Shapiro

Corey M. Shapiro
William E. Sharp
Bethany N. Baxter
ACLU of Kentucky Foundation
325 W. Main St. #2210
Louisville, KY 40202
(502) 581-9746
corey@aclu-ky.org
wsharp@aclu-ky.org
bbaxter@aclu-ky.org

Adriel I. Cepeda Derieux*
American Civil Liberties Union
Foundation 915 15th Street NW
Washington, DC 20005
(202) 457-0800
acepedaderieux@aclu.org

Theresa J. Lee*
Sophia Lin Lakin*
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
tlee@aclu.org
slakin@aclu.org

** application for admission pro hac vice forthcoming*

EXHIBIT 1

U.S. Department of Justice

Civil Rights Division

CONFIDENTIAL MEMORANDUM OF UNDERSTANDING

I. PARTIES & POINTS OF CONTACT.

Requester
Federal Agency Name: Civil Rights Division, U.S. Department of Justice
VRL/Data User: Eric Neff
Title: Acting Chief, Voting Section
Address: 150 M St. NE, Ste. 8-139, Washington DC 20002
Phone: (202) 704-5430

VRL/Data Provider
State Agency Name: Office of the Texas Secretary of State
Custodian: Adam Bitter
Title: General Counsel
Address: P.O. Box 12697, Austin, Texas 78711-2697
Phone: (512) 475-2813

The parties to this Memorandum of Understanding ("MOU" or "Agreement") are the Department of Justice, Civil Rights Division ("Justice Department" or "Department"), and the State of Texas ("Texas").

II. AUTHORITY.

By this Agreement, Texas has agreed to, and will, provide an electronic copy of your state's complete statewide Voter Registration List ("VRL" or "VRL/Data") to the Civil Rights Division of the U.S. Department of Justice (at times referred to as the "Department"). The VRL/Data must include, among other fields of data, the voter registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social

security number as required under the HAVA to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A).

The authorities by which this information is requested by the Department of Justice are:

- National Voter Registration Act of 1993, 52 U.S.C. § 20501, *et seq*.
- Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. See 52 U.S.C. § 20501(a).
- Help America Vote Act of 2002, 52 U.S.C. § 20901, *et seq.*
- Attorney General's authority to enforce the Help America Vote Act under 53 U.S.C. § 21111.
- Attorney General authority to request records pursuant to Title III of the Civil Rights Act of 1960 ("CRA"), codified at 52 U.S.C. § 20701, *et seq*.
- The Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

III. PURPOSE.

A VRL is a Voter Registration List pursuant to the NVRA and HAVA, commonly referred to as "voter roll," compiled by a state – often from information submitted by counties – containing a list of all the state's *eligible* voters. Regardless of the basis for ineligibility, ineligible voters do not appear on a state's VRL when proper list maintenance is performed by states. The Justice Department is requesting your state's VRL to test, analyze, and assess states' VRLs for proper list maintenance and compliance with federal law. In the event the Justice Department's analysis of a VRL results in list maintenance issues, insufficiency, inadequacy, anomalies, or concerns, the Justice Department will notify your state's point of contact of the issues to assist your state with curing.

The purpose of this MOU is to establish the parties' understanding as to the security protections for data transfer and data access by the Department of Justice of the electronic copy of the statewide voter registration list, including all fields requested by the Department of Justice.

IV. TIMING OF AGREEMENT – TIME IS OF ESSENCE.

Although the Justice Department is under no such obligation as a matter of law, because this Agreement is proposed, made, and to be entered into at your state's request as part of your state's transmission of its VRL to the Justice Department, this Agreement is to be fully executed within seven (7) days of the Justice Department presenting this Agreement to you. Both parties agree that no part of this Agreement or execution is intended to, or will, cause delay of the transmission of your state's VRL to the Justice Department for analysis.

V. TIMING OF VRL/DATA TRANSFER.

You agree to transfer an electronic copy of your state's complete statewide VRL/Data to the Civil Rights Division of the U.S. Department of Justice as described in Section III of this Agreement no later than five (5) business days from the execution of this Agreement, which is counted from the last day of the last signatory.

VI. METHOD OF VRL/DATA ACCESS OR TRANSFER.

The VRL will be submitted by your state via the Department of Justice's secure file-sharing system, i.e., Justice Enterprise File Sharing (JEFS"). A separate application to use JEFS must be completed and submitted by your state through the Civil Rights Help Desk. JEFS implements strict access controls to ensure that each user can only access their own files. All files and folders are tied to a specific user, and each user has defined permissions that govern how they may interact with those files (e.g., read, write, or read-only).

Whenever a user attempts to access a file or folder, JEFS validates the request against the assigned permissions to confirm that the user is explicitly authorized. This process guarantees that users can only access files and folders only where they have permission. Users are also limited to the authorized type of interaction with each file or folder. Within the Department of Justice, access to JEFS is restricted to specific roles: Litigation Support, IT staff, and Civil Rights Division staff.

VII. LOCATION OF DATA AND CUSTODIAL RESPONSIBILITY.

The parties mutually agree that the Civil Rights Division (also "Department") will be designated as "Custodian" of the file(s) and will be responsible for the observance of all conditions for use and for establishment and maintenance of security agreements as specified in this agreement to prevent unauthorized use. The information that the Department is collecting will be maintained consistent with the Privacy Act of 1974, 5 U.S.C. § 552a. The full list of routine uses for this collection of information can be found in the Systems of Record Notice ("SORN") titled, JUSTICE/CRT – 001, "Central Civil Rights Division Index File and Associated Records," 68 Fed. Reg. 47610-01, 611 (August 11, 2003); 70 Fed. Reg. 43904-01 (July 29, 2005); and 82 Fed. Reg. 24147-01 (May 25, 2017). It should be noted that the statutes cited for routine use include NVRA, HAVA, and the Civil Rights Act of 1960, and the Justice Department is making our request pursuant to those statutes. The records in the system of records are kept under the authority of 44 U.S.C. § 3101 and in the ordinary course of fulfilling the responsibility assigned to the Civil Rights Division under the provisions of 28 C.F.R. §§ 0.50, 0.51.

VRL/Data storage is similar to the restricted access provided on JEFS and complies with the SORN: Information in computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only a limited number of staff members who are assigned a specific identification code will be able to use the computer to access

the stored information. However, a section may decide to allow its employees access to the system in order to perform their official duties.

All systems storing the VRL data will comply with all security requirements applicable to Justice Department systems, including but not limited to all Executive Branch system security requirements (e.g., requirements imposed by the Office of Management and Budget [OMB] and National Institute of Standards and Technology [NIST]), Department of Justice IT Security Standards, and Department of Justice Order 2640.2F.

VIII. NVRA/HAVA COMPLIANT VOTER REGISTRATION LIST.

After analysis and assessment of your state's VRL, the Justice Department will securely notify you or your state of any voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, the Justice Department found when testing, assessing, and analyzing your state's VRL for NVRA and HAVA compliance, i.e., that your state's VRL only includes eligible voters.

You agree therefore that within forty-five (45) days of receiving that notice from the Justice Department of any issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, your state will clean its VRL/Data by removing ineligible voters and resubmit the updated VRL/Data to the Civil Rights Division of the Justice Department to verify proper list maintenance has occurred by your state pursuant to the NVRA and HAVA.

IX. CONFIDENTIALITY & DEPARTMENT SAFEGUARDS.

Any member of the Justice Department in possession of a VRL/Data will employ reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such data. Compliance with these safeguards will include secure user authentication protocols deploying either: (i) Two-Factor Authentication ("2FA"), which requires users to go through two layers of security before access is granted to the system; or (ii) the

assignment of unique user identifications to each person with computer access plus unique complex passwords, which are not vendor supplied default passwords.

The Department will activate audit logging for the records, files, and data containing the state's VRL/Data in order to identify abnormal use, as well as to track access control, on computers, servers and/or Devices containing the VRL/Data.

For all devices storing records, files, and data containing the VRL/Data: there is (i) up-to-date versions of system security agent software that includes endpoint protection and malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and (ii) up-to-date operating system security patches designed to maintain the integrity of the personal information.

For all devices storing records, files, and data containing the VRL/Data: there is (i) controlled and locked physical access for the Device; and (ii) the prohibition of the connection of the Device to public or insecure home networks.

There will be no copying of records, files, or data containing the VRL/Data to unencrypted USB drives, CDs, or external storage. In addition, the use of devices outside of moving the records, files, or data to the final stored device location shall be limited.

Any notes, lists, memoranda, indices, compilations prepared or based on an examination of VRL/Data or any other form of information (including electronic forms), that quote from, paraphrase, copy, or disclose the VRL/Data with such specificity that the VRL/Data can be identified, or by reasonable logical extension can be identified will not be shared by the Department. Any summary results, however, may be shared by the Department.

In addition to the Department's enforcement efforts, the Justice Department may use the information you provide for certain routine, or pre-litigation or litigation purposes including:

present VRL/Data to a court, magistrate, or administrative tribunal; a contractor with the Department of Justice who needs access to the VRL/Data information in order to perform duties related to the Department's list maintenance verification procedures. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(m).

X. LOSS OR BREACH OF DATA.

If a receiving party discovers any loss of VRL/Data, or a breach of security, including any actual or suspected unauthorized access, relating to VRL/Data, the receiving party shall, at its own expense immediately provide written notice to the producing party of such breach; investigate and make reasonable and timely efforts to remediate the effects of the breach, and provide the producing party with assurances reasonably satisfactory to the producing party that such breach shall not recur; and provide sufficient information about the breach that the producing party can reasonably ascertain the size and scope of the breach. The receiving party agrees to cooperate with the producing party or law enforcement in investigating any such security incident. In any event, the receiving party shall promptly take all necessary and appropriate corrective action to terminate unauthorized access.

XI. DESTRUCTION OF DATA.

The Department will destroy all VRL/Data associated with actual records as soon as the purposes of the list maintenance project have been accomplished and the time required for records retention pursuant to applicable law has passed. When the project is complete and such retention requirements by law expires, the Justice Department will:

1. Destroy all hard copies containing confidential data (e.g., shredding);
2. Archive and store electronic data containing confidential information offline in a secure location; and

3. All other data will be erased or maintained in a secured area.

XII. OTHER PROVISIONS.

A. Conflicts. This MOU constitutes the full MOU on this subject between the Department and your state. Any inconsistency or conflict between or among the provisions of this MOU, will be resolved in the following order of precedence: (1) this MOU and (2) other documents incorporated by reference in this MOU (e.g., transaction charges).

B. Severability. Nothing in this MOU is intended to conflict with current law or regulation or the directives of Department, or the your state. If a term of this MOU is inconsistent with such authority, then that term shall be invalid but, to the extent allowable, the remaining terms and conditions of this MOU shall remain in full force and effect.

C. Assignment. Your state may not assign this MOU, nor may it assign any of its rights or obligations under this MOU. To the extent allowable by law, this MOU shall inure to the benefit of, and be binding upon, any successors to the Justice Department and your state without restriction.

D. Waiver. No waiver by either party of any breach of any provision of this MOU shall constitute a waiver of any other breach. Failure of either party to enforce at any time, or from time to time, any provision of this MOU shall not be construed to be a waiver thereof.

E. Compliance with Other Laws. Nothing in this MOU is intended or should be construed to limit or affect the duties, responsibilities, and rights of the User Agency under the National Voter Registration Act, 52 U.S.C. § 20501 *et seq.*, as amended; the Help America Vote Act, 52 U.S.C. § 20901 *et seq.*, as amended; the Voting Rights Act, 52 U.S.C. § *10301 et seq.*, as amended; and the Civil Rights Act, 52 U.S.C. § 10101 et seq., as amended.

F. Confidentiality of MOU. To the extent allowed by applicable law, this MOU, its contents, and the drafts and communications leading up to the execution of this MOU are deemed

by the parties as "confidential." Any disclosures therefore could be made, if at all, pursuant to applicable laws or court orders requiring such disclosures.

SIGNATURES

VRL/Data Provider

State Agency Name: Office of the Texas Secretary of State

Signature: _____ Date of Execution: 12/5/25

Authorized Signatory Name Printed: Adam Bitter

Title: General Counsel

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

Signature: _____ Date of Execution: 12/9/2025

Authorized Signatory Name Printed: Eric Neff

Title: Acting Chief, Voting Section, Civil Rights Division