NO. 20-55175, 20-55252

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

GERARDO GONZALEZ, *et al.*,

PLAINTIFFS-CROSS-APPELLANTS/APPELLEES,

V.

IMMIGRATION AND CUSTOMS ENFORCEMENT, *et al.*,

DEFENDANTS-CROSS-APPELLANTS/APPELLEES

On Appeal from the United States District Court
District for Central California, Los Angeles
2:13-cv-04416-AB-FFM

The Honorable Andre Birotte, Jr., District Judge

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFFS-CROSS-APPELLANTS/APPELLEES AND AFFIRMANCE

Saira Hussain
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Fax.: (415) 436-9993
Email: saira@eff.org

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amicus curiae Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10 percent or more of its stock.

Dated: June 11, 2020

By: /s/ *Saira Hussain*
Saira Hussain

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT i

TABLE OF CONTENTS ii

TABLE OF AUTHORITIES iv

STATEMENT OF INTEREST 1

INTRODUCTION 2

ARGUMENT..3

I. THE FOURTH AMENDMENT REQUIRES THAT LAWFUL SEARCHES OR SEIZURES BE PREMISED ON RELIABLE INFORMATION. 3

II. WHEN LAW ENFORCEMENT RELIES ON TECHNOLOGY LIKE DATABASES TO ESTABLISH PROBABLE CAUSE, COURTS REQUIRE SAFEGUARDS TO ENSURE THE RELIABILITY OF THE INFORMATION USED—SAFEGUARDS THAT ARE NOT PRESENT HERE...6

A. Analogous technologies require safeguards such as industry-accepted tests, independent certifications, or audits to be reliable for probable cause. 6

B. Unlike drug-sniffing dogs, computer software, and breathalyzers, ICE databases are not subject to independent testing, certification, or audits, which underscores their unreliability...9

C. The federal government shields the vast majority of the databases ICE uses from the accuracy, transparency, and privacy requirements of the Privacy Act, further undermining the reliability of the databases. 11

1. The databases ICE relies on for removability determinations are exempt from accuracy and accountability requirements of the Privacy Act. 12

2. ICE's choice to rely on a labyrinth of systems for removability determinations makes it impossible to track data flows and ensure record accuracy. 15

III. ICE'S USE OF DATABASES BEYOND THEIR INTENDED PURPOSES YIELDS UNRELIABLE RESULTS. 19

IV. BECAUSE ICE'S DATABASES LACK SAFEGUARDS AND ARE USED FAR BEYOND THEIR INTENDED PURPOSES, THEY CANNOT PROVIDE PROBABLE CAUSE OF REMOVABILITY. 23

CONCLUSION 25

CERTIFICATE OF COMPLIANCE...26

CERTIFICATE OF SERVICE...27

TABLE OF AUTHORITIES

Cases

Alabama v. White,
496 U.S. 325 (1990) 23

Arcia v. Florida Secretary of State,
772 F.3d 1335 (11th Cir. 2014) 19, 20, 21

Arizona v. Evans,
514 U.S. 1 (1995) 3

Coolidge v. New Hampshire,
403 U.S. 443 (1971) 4

Dunaway v. New York,
442 U.S. 200 (1979) 5

Florida v. Harris,
568 U.S. 237 (2013) 7, 23

Florida v. Jardines,
569 U.S. 1 (2013) 7

Henry v. United States,
361 U.S. 98 (1959) 5

Herring v. United States,
555 U.S. 135 (2009) 4

Illinois v. Gates,
462 U.S. 213 (1983) 5, 23, 24

Jones v. United States,
357 U.S. 493 (1958) 4

League of United Latin Am. Citizens v. Wilson,
908 F. Supp. 755 (C.D. Cal. 1995) 22, 23

Michigan v. Summers,
452 U.S. 692 (1981) 3, 4

Millender v. County of Los Angeles,
620 F.3d 1016 (9th Cir. 2010) 19, 20

Montana Immigrant Justice Alliance v. Bullock,
371 P.3d 430 (Mont. 2016) 21, 22, 23

State v. Conley,
No. 48-2012-CT-000017-A/A (Fla. Cir. Ct. 2014) 9

State v. Garcia,
No. 12-CT-800 (Fla. Cir. Ct. 2012) 9

Tejada-Mata v. INS,
626 F.2d 721 (9th Cir. 1980) 4

United States v. Esquivel-Rios,
725 F.3d 1231 (10th Cir. 2013) 6, 24

United States v. Jordan,
No. 2:19-cr-125 (D. Utah 2020) 7

United States v. Ludwig,
641 F.3d 1243 (10th Cir. 2011) 7

United States v. Thomas,
788 F.3d 345 (2d Cir. 2015) 8, 24

United States v. United States Dist. Ct. for the Eastern Dist. of Michigan,
407 U.S. 297 (1972) 4

Villas at Parkside Partners v. City of Farmers Branch, Texas,
726 F.3d 524 (5th Cir. 2013) 21

Whiteley v. Warden, Wyoming State Penitentiary,
401 U.S. 560 (1971) 5

Statutes

5 U.S.C. § 552a .... *passim*

6 U.S.C. § 142 12

Legislative Materials

S. Rep. No. 93-1183 12

U.S. Government Accountability Office, Testimony Before the Subcommittee on Immigration and National Interest, Committee on the Judiciary, U.S. Senate, *Border Security: Actions Needed by DHS to Address Long-Standing Challenges in Planning for a Biometric Exit System* (Jan. 20, 2016)....................................10

Other Authorities

Alex Newman, *This Is the Data We No Longer Get about Immigration Enforcement under the Trump Administration*, The World (Mar. 30, 2017) 16

Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* (MIT 1973)..15, 18

DHS/CBP/PIA-024 Arrival and Departure Information System (Jan. 2020).........17

DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 Fed. Reg. 69984 (Nov. 21, 2013) 13, 14, 18

DHS/USCIS/PIA-009(a) Privacy Impact Assessment for the Central Index System (CIS) (Apr. 7, 2017)...17, 18

DHS/USCIS-011 TECS System of Records, 74 Fed. Reg. 45072 (Aug. 31, 2009) 14

ICE Student and Exchange Visitor Information System (SEVIS) of Records, 73 Fed. Reg. 63058 (Oct. 23, 2008)..14

Joan Friedland, *Untangling the Immigration Enforcement Web*, Nat'l Immigration Law Ctr. (Sept. 2017)...16

LaFave, Search and Seizure: A Treatise on the Fourth Amendment, § 3.4 (2019).. 5

Stacy Cowley & Jessica Silver-Greenberg, *These Machines Can Put You in Jail. Don't Trust Them.*, N.Y. Times (Nov. 3, 2019) 8, 9

STATEMENT OF INTEREST[1]

Amicus curiae Electronic Frontier Foundation is a member-supported, non-profit civil liberties organization that has worked for 30 years to ensure that technology supports freedom, justice, and innovation for all people of the world. With over 30,000 members, EFF represents the interests of those impacted by technologies both in court cases and broader policy debates, and actively encourages and challenges the government and courts to support privacy and safeguard individual autonomy to ensure that new technologies enhance civil liberties rather than abridge them.

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(c), EFF certifies that no person or entity, other than amicus curiae, its members, or its counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. The parties have consented to the filing of this brief.

INTRODUCTION

Immigration and Customs Enforcement (ICE) agents rely on a network of databases to make life-changing decisions: whether to authorize a person's warrantless arrest to initiate deportation proceedings. ICE agents issue these immigration detainers without ever interviewing the person, conducting further investigation beyond the databases, or seeking neutral review of probable cause. The databases serve as the first, last, and *only* indications of removability.

These databases, however, are unreliable in a multitude of ways. The district court identified some: namely, that the databases are full of errors, provide static information about dynamic facts, are materially incomplete, and were never intended to be used to make probable cause determinations of removability.

But the databases are unreliable for additional reasons, as well. ICE does not subject the databases on which it relies to any industry-accepted tests, independent certifications, or even periodic audits—safeguards courts require for analogous technologies to be sufficiently reliable for probable cause determinations. Additionally, the federal government shields the vast majority of the databases ICE uses from the accuracy, transparency, and privacy requirements of the federal Privacy Act, 5 U.S.C. § 552a, further undermining efforts to hold ICE—and the databases it relies on—accountable.

In addition to these persistent problems, other courts in a variety of different contexts have recognized that use of databases beyond their intended purposes yields unreliable results.

The Fourth Amendment requires probable cause based on reasonably trustworthy information to believe that wrongdoing has occurred. *Michigan v. Summers*, 452 U.S. 692, 700 (1981). ICE's network of databases falls far short of this constitutional mandate.

The district court's judgment puts into place meaningful and desperately needed limits to ensure that ICE is not exempt from the Fourth Amendment. Amicus urges this Court to affirm the district court and uphold the injunction prohibiting ICE from issuing warrantless immigration detainers based solely on its network of databases.

ARGUMENT

I. THE FOURTH AMENDMENT REQUIRES THAT LAWFUL SEARCHES OR SEIZURES BE PREMISED ON RELIABLE INFORMATION.

Where the government relies on technology—like the databases at issue here—to establish probable cause to constrain a person's liberty, the Fourth Amendment requires that the technology be trustworthy. *See Arizona v. Evans*, 514 U.S. 1, 17 (1995) (O'Connor, J. concurring) ("Surely it would *not* be reasonable for the police to rely, say, on a recordkeeping system . . . that has no mechanism to ensure its accuracy over time and that routinely leads to false arrests"); *Herring v. United States*, 555 U.S. 135, 146 (2009) ("In a case where systemic errors were demonstrated, it might be reckless for officers to rely on an unreliable warrant system").

The Fourth Amendment prohibits unreasonable searches and seizures. U.S. Const. amend. IV. The "most basic constitutional rule" under the Fourth Amendment is that warrantless searches and seizures—those accomplished "outside the judicial process, without prior approval by judge or magistrate"—are presumptively unconstitutional. *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971) (internal quotations and citations omitted).

Obtaining a warrant—issued by a neutral and detached magistrate, satisfying the familiar requirements of probable cause and particularity—is the "time-tested means" for protecting Fourth Amendment rights. *United States v. United States Dist. Ct. for the Eastern Dist. of Michigan*, 407 U.S. 297, 318 (1972). This most-basic rule is subject only to a few "jealously and carefully drawn" exceptions. *Jones v. United States*, 357 U.S. 493, 499 (1958). For example, a warrantless arrest can nonetheless be constitutional, but only if based upon probable cause and reviewed promptly by a neutral magistrate. *Summers*, 452 U.S. at 700; *see also Tejada-Mata v. INS*, 626 F.2d 721, 724-25 (9th Cir. 1980) (applying probable cause standard to immigration arrests).

Whether in support of a warrant or a warrantless arrest, probable cause cannot be established through "common rumor or report, suspicion, or even [an officer's] strong reason to suspect" that a violation has been committed. *Henry v. United States*, 361 U.S. 98, 101 (1959) (internal quotation and citation omitted).

Instead, probable cause requires objective and *reliable* evidence of an offense. *Dunaway v. New York*, 442 U.S. 200, 208 n. 9 (1979). And, in a variety of contexts, courts scrutinize the reliability of information on which law enforcement makes probable cause determinations. For example, when law enforcement relies on an informant to support probable cause, the informant's veracity, reliability, and basis of knowledge are "closely intertwined issues that may usefully illuminate the common-sense, practical question [of] whether there is probable cause." *Illinois v. Gates*, 462 U.S. 213, 230 (1983). Even information provided by another law enforcement officer or the victim of a crime must nonetheless be evaluated for reliability. *See Whiteley v. Warden, Wyoming State Penitentiary*, 401 U.S. 560, 565 (1971) (finding Fourth Amendment violation where the arrest was based solely on a defective warrant obtained and disseminated by another law enforcement agency); *see also* LaFave, Search and Seizure: A Treatise on the Fourth Amendment, § 3.4 (2019).

These Fourth Amendment mandates, as the district court below noted, "serve[] an exceedingly important function in the immigration context," as "many of the backstops that exist in the criminal justice system are absent in the immigration system." ER 39.

II. WHEN LAW ENFORCEMENT RELIES ON TECHNOLOGY LIKE DATABASES TO ESTABLISH PROBABLE CAUSE, COURTS REQUIRE SAFEGUARDS TO ENSURE THE RELIABILITY OF THE INFORMATION USED—SAFEGUARDS THAT ARE NOT PRESENT HERE.

The Fourth Amendment requires that the databases ICE uses are reliable. *United States v. Esquivel-Rios*, 725 F.3d 1231, 1236-38 (10th Cir. 2013) (Gorsuch, J.). But unlike analogous technologies—which require industry-accepted examinations, independent certifications, or audits to be deemed reliable—the databases upon which ICE relies for its removability determinations are subject to far less scrutiny. Moreover, these databases are expressly exempt from accuracy, completeness, and transparency requirements under the federal Privacy Act, which further casts doubt on their reliability.

A. Analogous technologies require safeguards such as industry-accepted tests, independent certifications, or audits to be reliable for probable cause.

When law enforcement relies on new technology to support probable cause, courts insist on industry-accepted examinations, independent certifications, or frequent audits to establish the reliability of that technology.

For instance, canines used for drug detection are treated like a type of sense-enhancing technology and provide a particularly well-developed example of the criteria courts apply. *See Florida v. Jardines*, 569 U.S. 1, 12-13 (2013) (Kagan, J., concurring) ("drug-detection dogs are highly trained tools of law enforcement"). In *Florida v. Harris*, the Supreme Court held that "evidence of a dog's satisfactory performance in a certification or training program can provide sufficient reason to trust his alert" and, thus, provide a reliable basis for probable cause. 568 U.S. 237, 246-47 (2013). *Accord United States v. Ludwig*, 641 F.3d 1243, 1251 (10th Cir. 2011) ("courts typically rely on the dog's certification"); *United States v. Jordan*, No. 2:19-cr-125, at *13 (D. Utah 2020) ("courts have consistently recognized that the training necessary to support certification must be completed successfully, that the certification must be current and updated through ongoing training, and that both must be supported by accurate and timely kept records").

Notwithstanding a drug-detection dog's independent training and certification, a defendant can still challenge a finding of probable cause by questioning the adequacy of a certification or training program. *Harris*, 568 U.S. at 247. *See also Jordan*, No. 2:19-cr-125, at *13-15 (ruling a dog sniff unreliable in part because of the state training program's "failure to implement double-blind training").

Courts have applied analogous criteria to the use of specific computer software to establish probable cause. Software does not provide a reliable basis for establishing probable cause where it "report[s] false or misleading information" or where there are "industry-accepted tests or methodology" that could have been used, but were not used, to enhance the software's reliability. *United States v. Thomas*, 788 F.3d 345, 353 (2d Cir. 2015) (affirming district court's finding that software was reliable).

Recently, several states have questioned the reliability of portable machines used to detect blood alcohol content.[2] In Massachusetts and New Jersey alone, judges declared inadmissible more than 30,000 alcohol breath tests between 2018 and 2019 because of their lack of reliability.[3] An analyst for the Washington, D.C., Metropolitan Police Department discovered, upon examining department alcohol breath-testing devices, that the machines had been generating results that were 20 to 40 percent too high.[4]

One Florida court, addressing the reliability of alcohol breath-testing devices, concluded that, although the devices functioned correctly 80 percent of the

[2] These challenges generally arise in the context of evidentiary admissibility rather than probable cause. However, the machine's reading often serves as a basis for probable cause of arrest *and* the key evidence for a conviction. *State v. Conley*, No. 48-2012-CT-000017-A/A, at *24 (Fla. Cir. Ct. 2014) ("in DUI trials, where the operation of a motor vehicle is rarely at issue, a breath test greater than .08 is tantamount to telling the jury to convict the defendant"). *Available at* https://int.nyt.com/data/documenthelper/1935-orange-county-decision-2014-breath-tests/d785cd5b0e65bdc10755/optimized/full.pdf#page=1.

[3] Stacy Cowley & Jessica Silver-Greenberg, *These Machines Can Put You in Jail. Don't Trust Them.*, N.Y. Times (Nov. 3, 2019), https://www.nytimes.com/2019/11/03/business/drunk-driving-breathalyzer.html.

[4] *Id.*

time, the fact that the device "mostly works" is an "insufficient response when a citizen's liberty is at risk." *State v. Conley*, No. 48-2012-CT-000017-A/A, at *24 (Fla. Cir. Ct. 2014). *See also State v. Garcia*, No. 12-CT-800, at *4 (Fla. Cir. Ct. 2012).[5] The court deemed the device nothing more than "a magic black box assisting the prosecution in convicting citizens of DUI," *Conley*, at *24; several Florida judges have rejected the admission of breath-test results altogether.[6]

B. Unlike drug-sniffing dogs, computer software, and breathalyzers, ICE databases are not subject to independent testing, certification, or audits, which underscores their unreliability.

The databases ICE relies on have none of the requisite safeguards to reliably establish probable cause. There are no industry-accepted studies, independent certifications, or audits of any sort that speak to the reliability of ICE's databases for probable cause determinations. *See* Plaintiffs/Cross-Appellants Br. at 24-25 (citing to testimony of Homeland Security and ICE officials indicating they lack knowledge of the reliability of their databases).

In fact, independent investigations of several databases ICE uses have highlighted the *unreliability* of their information. In 2017, the U.S. Department of Homeland Security (DHS) Office of the Investigator General (OIG) found that one

[5] *Available at* https://int.nyt.com/data/documenthelper/1919-florida-carr-2012-ruling/d785cd5b0e65bdc10755/optimized/full.pdf#page=1.

[6] *See* Cowley & Silver-Greenberg, *supra* note 3.

database, the Arrival and Department Information System (ADIS), incorrectly identified visa overstays more than 42 percent of the time. ER 31. In 2012, a DHS OIG report found that in the Central Index System (CIS) database, the class of admission (i.e. the person's citizenship and/or immigration status at the time they were admitted to the United States) was incorrect for 12 percent of individuals studied. ER 28. And in 2016, the Government Accountability Office (GAO) stated that DHS had not reported annual visa overstay rates to Congress since 1994 "[b]ecause of concerns about the reliability of the department's overstay data" contained in its TECS database.[7]

These error-ridden databases then feed into ICE's automated process to determine removability. The Alien Criminal Response Information Management System (ACRIMe) includes a web-based interface that automatically reviews information stored within ten databases. ER 24. Based on that information, ACRIMe generates a short statement, known as an Immigrant Alien Response (IAR), which consists of basic biographic data and limited information about

[7] U.S. Government Accountability Office, Testimony Before the Subcommittee on Immigration and National Interest, Committee on the Judiciary, U.S. Senate, *Border Security: Actions Needed by DHS to Address Long-Standing Challenges in Planning for a Biometric Exit System* (Jan. 20, 2016), https://www.gao.gov/assets/680/674704.pdf (listed as exhibit 236 in SER 228).

immigration status and removability. ER 24. Often, analysts rely *solely* on the IAR to recommend issuance of an immigration detainer. ER 24-25.

Given the unreliability of ICE's system of databases, using the IAR to issue immigration detainers is akin to reliance on a "magic black box." However, even if analysts were to look past this initial determination and review the databases themselves, they likely would *still* end up with an erroneous determination of removability because the errors stem from the underlying data. *See* ER 25.

An individual's liberty cannot hinge upon the contents of an opaque network of databases that is only accurate some of the time.

C. The federal government shields the vast majority of the databases ICE uses from the accuracy, transparency, and privacy requirements of the Privacy Act, further undermining the reliability of the databases.

The federal Privacy Act, 5 U.S.C. § 552a, requires all federal agencies to maintain accurate records on individuals. However, despite this clear legal mandate and despite years of demonstrated database errors, ICE and other DHS components routinely exempt their databases from key accountability measures in the Privacy Act. In addition, these databases have complex and often untraceable data flows, which increase the probability that errors will reoccur in the future. These two issues further compound the problems discussed above and show that the information in these databases cannot be relied upon to support probable cause under the Fourth Amendment.

1. The databases ICE relies on for removability determinations are exempt from accuracy and accountability requirements of the Privacy Act.

The databases relied on by ICE to make removability determinations are full of inaccuracies. Despite this, DHS and its component agencies universally exempt their databases from key provisions of the Privacy Act that could prevent or at least mitigate this problem.

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government." S. Rep. No. 93-1183 at 1. The Homeland Security Act of 2002, which established DHS, specifically calls on DHS's Chief Privacy Officer to assure that DHS's use of technologies "sustains, and do[es] not erode, privacy protections" and ensure that all personal information held in DHS systems of records "is handled in full compliance with fair information practices as set out in the Privacy Act of 1974." 6 U.S.C. § 142.

One of the most important of these fair information practices requires that agencies "[m]aintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." 5 U.S.C. § 552a(e)(5).

Nevertheless, DHS and its component agencies have chosen to exempt their systems from numerous Privacy Act mandates. For example, U.S. Citizenship and Immigration Services (USCIS), the agency that maintains the CIS database, exempts CIS from a laundry list of Privacy Act provisions.[8] Among these exceptions is 5 U.S.C. § 552a(e)(1), which requires that a system of records contain "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency[.]" *Id.* at § 552a(e)(1). In addition, agencies need not comply with 5 U.S.C. § 552a(e)(5)'s "accuracy, relevance, timeliness, and completeness" requirements for records within CIS.[9]

CIS is not unique. TECS, another system relied on by ICE, is a "repository of information" maintained by DHS and used in civil and criminal investigations, inquiries, and proceedings as well as to aid national security and intelligence

[8] "The Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2): 5 U.S.C. 552a(c)(3) and (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (e)(12), (f), (g)(1), and (h). Additionally, the Secretary of Homeland Security has exempted this system from the following provisions of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2): 5 U.S.C. 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f)." DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 78 Fed. Reg. 69984 (Nov. 21, 2013), https://www.govinfo.gov/content/pkg/FR-2013-11-22/html/2013-27896.htm

[9] *See* Alien File, Index, and National File Tracking System of Records, *supra* note 8.

activities.[10] DHS has exempted TECS from the Privacy Act's notice and access requirements; purpose limitations on the use of personal information; and any accuracy, relevance, timeliness, or completeness requirements.[11] SEVIS, a database of student visa holders that ICE reviews in making removability determinations, is similarly exempt from purpose limitations on the use of personal information and notice and access requirements.[12]

Not only does DHS exempt its databases from accuracy, relevancy, and transparency requirements, it also exempts many of them from the Privacy Act's right to a civil remedy for agency violations of the Act under 5 U.S.C. § 552a(g).[13] Therefore, individuals have no recourse even when they discover their files are inaccurate.

[10] DHS/USCIS-011 TECS System of Records, 74 Fed. Reg. 45072 (Aug. 31, 2009), https://www.govinfo.gov/content/pkg/FR-2009-08-31/html/E9-20765.htm.

[11] TECS is exempt from 5 U.S.C. §§ 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5) and (e)(8); (f), and (g) pursuant to 5 U.S.C. § 552a(j)(2) and from 5 U.S.C. §§ 552a (c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), (e)(4)(I), and (f) pursuant to 5 U.S.C. § 552a(k)(2). *Id.*

[12] SEVIS is exempt from 5 U.S.C. §§ 552a(c)(3); (d); (e)(1); (e)(4)(G), (H) and (I). ICE Student and Exchange Visitor Information System (SEVIS) of Records, 73 Fed. Reg. 63058 (Oct. 23, 2008), https://www.govinfo.gov/content/pkg/FR-2008-10-23/html/E8-25000.htm.

[13] *See* Alien File, Index, and National File Tracking System of Records, *supra* note 8; TECS System of Records, *supra* note 10.

The fact that the databases ICE relies upon to make its removability decisions are exempt from key requirements of the Privacy Act means that ICE has no incentive to improve the accuracy of its records. This further supports the district court's determination that these databases do not provide a reliable basis for probable cause determinations.

2. ICE's choice to rely on a labyrinth of systems for removability determinations makes it impossible to track data flows and ensure record accuracy.

Despite Congress's best efforts, in passing the Privacy Act, to require agencies to protect individuals' data, the way DHS and its components like ICE have chosen to collect, organize, and share data makes it virtually impossible for the agencies to comply with the Privacy Act's mandates.

ICE relies on a dizzying array of databases to try to determine individuals' removability. ER 25-27. Because each of the databases that ICE uses receives data from, and distributes data to, multiple sources, ICE does not have effective control over the accuracy of all the information in its files.[14]

[14] This was a key problem of many databases noted by the 1972 Advisory Committee whose findings led to the creation of the Privacy Act. *See* Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* 17-18 (MIT 1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf (copy of original) (finding, with respect to earlier databases, that where a system is "essentially an automated receiver, searcher, and distributor of data furnished by others" the system owner cannot control the accuracy of the records).

This becomes clear when one tries to map the databases ICE uses to issue detainers. The Privacy Act requires federal agencies to describe all of their databases that maintain records on individuals in System of Records Notices (SORNs). Each SORN describes the types of information contained in the database, the legal authority for collecting and maintaining the records, how the records are used within the agency, and the purposes (referred to as "routine uses") for which the agency may disclose the records to other parties without the individual record subject's consent. SORNs must be published in the Federal Register and made available to the public on the Internet.

Despite these transparency requirements, it is increasingly difficult to use SORNs to track data flows and to create a comprehensive list of databases an agency, like ICE, relies on to make life-changing decisions about individuals, such as removability.[15] The facts of this case exemplify the problem.

For example, one of the databases on which ICE relies, ADIS, is maintained by Customs and Border Protection (CBP). ER 26, 31. CBP describes ADIS as the

[15] *See* Joan Friedland, *Untangling the Immigration Enforcement Web*, at 23, Nat'l Immigration Law Ctr. (Sept. 2017), https://www.nilc.org/wp-content/uploads/2017/09/Untangling-Immigration-Enforcement-Web-2017-09.pdf; *see also* Alex Newman, *This Is the Data We No Longer Get about Immigration Enforcement under the Trump Administration*, The World (Mar. 30, 2017), https://www.pri.org/stories/2017-03-30/data-we-no-longer-get-about-immigration-enforcement-under-trump-administration.

"primary CBP system used to determine person-centric travel history and immigration status."[16] Although ADIS itself is a system of records, it also "consolidates data from a variety of [other] systems."[17] Therefore, to even begin to understand where the data that goes into ADIS comes from, how it is maintained, and with whom it is shared, one must also consult SORNs for six other systems.[18]

Similarly, as previously mentioned, ICE consults CIS for its removability determinations. ER 25, 27-30. This database is maintained by USCIS and is a "DHS-wide index used to track the location of case files . . . and to maintain alien status and repository information."[19] CIS contains information on many different classes of people, "including lawful permanent residents, naturalized citizens, U.S. border crossers, apprehended aliens, legalized aliens, aliens who have been issued employment authorizations, and other individuals of interest to DHS."[20]

[16] DHS/CBP/PIA-024 Arrival and Departure Information System (Jan. 2020), https://www.dhs.gov/publication/arrival-and-departure-information-system.

[17] *Id.*

[18] *Id.* (listing six additional associated SORNs).

[19] DHS/USCIS/PIA-009(a) Privacy Impact Assessment for the Central Index System (CIS), at 1 (Apr. 7, 2017), https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-09-a-cis-april-2017.pdf.

[20] *Id.*

Yet CIS does not have its own SORN. Instead, information in CIS is covered by the Alien File, Index, and National File Tracking System of Records.[21] In addition, CIS collects data from many other databases, including eight systems within USCIS, nine systems from other DHS components, and an additional three systems from external sources—in total 20 other systems.[22]

These complex and confusing systems make it virtually impossible for the public to track data flows and understand what data is collected and how that data is being used. These systems in their current form also make it virtually impossible for ICE to ensure the records upon which it makes life-changing decisions are accurate.[23] This increases the likelihood of unfair or inappropriate decisions about the individual to whom any given record pertains as well as the risk of unjust treatment by users of the system.

Overall, ICE chooses to rely on an inscrutable web of databases to make probable cause determinations. The government chooses to exempt that web of databases from federal laws that would help ensure the integrity and reliability of its data. And ICE chooses not to have the databases independently audited and

[21] *Id.* at 8 ("What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?"); *see also* Alien File, Index, and National File Tracking System of Records, *supra* note 8.

[22] Privacy Impact Assessment for CIS*, supra* note 19, at 3-6.

[23] *See supra* note 14.

certified—as is commonly required for law enforcement use of other technologies. Those choices render the databases ICE uses unreliable for probable cause determinations under the Fourth Amendment.

III. ICE'S USE OF DATABASES BEYOND THEIR INTENDED PURPOSES YIELDS UNRELIABLE RESULTS.

ICE's issuance of detainers in reliance on databases that were not designed for this purpose creates a "foreseeable risk of false positives and mismatches" that violates a person's right to be free from unreasonable seizures. *See Arcia v. Florida Secretary of State*, 772 F.3d 1335, 1342 (11th Cir. 2014). Just as databases are only as reliable as the information that goes into them, databases used beyond their intended purposes often yield unreliable results. In a variety of contexts outside of the Fourth Amendment, courts recognize that databases can be unreliable when used for purposes beyond their design.

In *Millender v. County of Los Angeles*, this Court rejected reliance on a state database to establish a fact that the database was not intended to address. 620 F.3d 1016 (9th Cir. 2010)) (en banc), *rev'd on other grounds sub nom. Messerschmidt v. Millender*, 565 U.S. 535 (2012). The court examined the sufficiency of a warrant that authorized the collection of firearms and gang-related items from a suspect's home. *Id.* at 1031. The court dismissed a contention that the magistrate could have inferred the suspect's criminal record based on the suspect's inclusion in the state's gang database. *Id.* at 1029 n.7. The database's own advisory committee warned that the database was "not designed to provide users with information upon which official actions may be taken" and further could not "be used to provide probable cause for an arrest or be documented in an affidavit for a search warrant" because names could be added to the database simply because the person had been seen "frequenting gang areas" or "affiliating with gang members." *Id.* (internal citations omitted). Thus, inclusion in the state's gang database could not provide a magistrate with reliable evidence to infer the suspect's prior criminal history. *Id.*

In *Arcia*, the Eleventh Circuit considered two programs enacted by the Florida Secretary of State to purge the voter rolls of ineligible non-citizens. 772 F.3d at 1338. The first program relied upon state motor vehicle records to determine voter eligibility. *Id.* at 1339. The second program superseded the first program, and relied on the federal Systemic Alien Verification for Entitlements (SAVE) database to determine eligibility. *Id.* at 1339-40. Plaintiffs, including two naturalized U.S. citizens, sued under the National Voter Registration Act (NVRA), which prohibits programs that systematically remove the names of ineligible voters from the voter rolls within 90 days of an election. *Id.* at 1338, 1340. The court found that the plaintiffs had standing—even though they had only been identified as non-citizens under the first program and were ultimately able to vote—because "there was a realistic probability that they would be misidentified due to unintentional mistakes in the Secretary's data-matching process." *Id.* at 1340-41.

The court further found that "the process of matching voters across various databases creates a foreseeable risk of false positives and mismatches based on user errors, problems with the data-matching process, flaws in the underlying databases, and similarities in names and birthdates." *Id.* at 1342. Accordingly, the court reversed the district court's grant of summary judgment for defendants and found Secretary of State violated the NVRA. *Id.* at 1348.

The Fifth Circuit addressed a similar issue in *Villas at Parkside Partners v. City of Farmers Branch, Texas*, 726 F.3d 524 (5th Cir. 2013). There, a city ordinance required individuals to obtain a license indicating they were "lawfully present" in the United States before renting an apartment or home. *Id.* at 526-27. The city relied on the SAVE database to determine who was "lawfully present." *Id.* at 533. However, SAVE "can provide only a non-citizen's specific immigration status; it does not answer lawful presence or not." *Id.* (internal quotations omitted). Without a database the city could use to reliably determine whether a non-citizen was lawfully present, the court found the ordinance was likely to lead to the "unnecessary harassment" of some immigrants. *Id.* at 534-35 (*citing United States v. Arizona*, 567 U.S. 387, 408 (2012)) (striking down the rule on preemption grounds).

The Montana Supreme Court confronted a similar situation in *Montana Immigrant Justice Alliance v. Bullock*, 371 P.3d 430 (Mont. 2016). There, the state legislature passed a law denying state-funded services to individuals deemed "illegal aliens" by relying on determinations informed by the SAVE database. *Id.* at 434-35. The court pointed out that a determination of unlawful entry or presence was required in order for a state official to determine if an individual was an "illegal alien," "but that determination cannot be made solely by querying the SAVE database." *Id.* at 442. Accordingly, the court found the statute "'incurs the risk that inconsistent and inaccurate judgments will be made'" and struck it down on preemption grounds. *Id.* (citing *League of United Latin Am. Citizens v. Wilson*, 908 F. Supp. 755, 770 (C.D. Cal. 1995)).

Here, like the databases in the cases discussed above, ICE's use of database information "deviates from the purpose for which those databases were designed." ER 46. For example, consider the CLAIMS 3 database: the database functions as a case processing and management system for USCIS and provides information on the adjudication of immigration applications and any credentials that resulted from the adjudication. ER 25-26. Because it was designed as a case management system, it destroys information after 15 years, as there is no need to maintain old applications on adjudicated benefits. ER 30. However, once ICE uses CLAIMS 3 for purposes of determining removability, the 15-year retention period serves as a significant limitation, since the database has no record of individuals who obtained lawful status more than 15 years ago, and thus may incorrectly identify them as removable. ER 30-31. The database's use for a purpose it was not designed to support is to blame for its high error rate. ER 30.

Thus, every time an ICE agent issues a detainer based solely on information in a database intended for another purpose, that agent "'incurs the risk that inconsistent and inaccurate judgments will be made.'" *See Montana Immigrant Justice Alliance*, 371 P.3d at 442 (citing *League of United Latin Am. Citizens*, 908 F. Supp. at 770).

IV. BECAUSE ICE'S DATABASES LACK SAFEGUARDS AND ARE USED FAR BEYOND THEIR INTENDED PURPOSES, THEY CANNOT PROVIDE PROBABLE CAUSE OF REMOVABILITY.

Probable cause requires an "balanced assessment of the relative weights of all the various indicia of reliability," where "a deficiency in one [area] may be compensated for . . . by a strong showing as to the other." *Gates*, 462 U.S. at 233-34. Both quantity—meaning the volume of information possessed by law enforcement—and quality—meaning the degree of reliability of the information—are important to this assessment. *Alabama v. White*, 496 U.S. 325, 330 (1990) (citations omitted).

The Government argues that probable cause for immigration detainers must be assessed on an individual basis because "even if the database alone is unreliable, the database search is but one part of the 'totality-of-the-circumstances analysis.'" Gov. Br. at 34-35 (citing *Harris*, 568 U.S. at 244).

But for the class in this case, there can be no "balanced assessment of the relative weights of all the various indicia of reliability" precisely because ICE agents rely *solely* on the databases to issue the immigration detainer. *See Gates*, 462 U.S. at 234. From a quantity perspective, there is limited information available to an analyst tasked with providing a removability recommendation. This information consists of ACRIMe's automated IAR and the underlying databases, as well as a handful of other databases that "provide extremely limited information," contain "no information" after 1995, or only summarize information in other databases. ER 24-26 & n.12. From a quality perspective, there is ample evidence that the databases ICE uses are unreliable because they lack safeguards and are not used for their intended purposes. *See supra* Part II-III.

Simply put, the databases alone comprise the totality of the circumstances ICE relies on to determine removability for the class members in this case. That may be sufficient where the technology previously has proven reliable, been independently certified, or otherwise been vetted for accuracy. *See Thomas*, 788 F.3d at 353. Here, however, ICE's databases do not meet these criteria and thus cannot be relied upon for probable cause. *See Esquivel-Rios*, 725 F.3d 1231, 1236-38.

CONCLUSION

For the foregoing reasons, this Court should affirm the district court's decision.

Dated: June 11, 2020

Respectfully submitted,

/s/ *Saira Hussain*

Saira Hussain
Jennifer Lynch
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
saira@eff.org

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(B), I certify as follows:

1. This Brief of Amicus Curiae Electronic Frontier Foundation in Support of Plaintiffs-Cross-Appellants/Appellees and Affirmance complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5,302 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: June 11, 2020

By: /s/ *Saira Hussain*
Saira Hussain

Counsel for Amicus Curiae
Electronic Frontier Foundation

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on June 11, 2020.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: June 11, 2020

By: /s/ *Saira Hussain*
Saira Hussain

Counsel for Amicus Curiae
Electronic Frontier Foundation