No. 14-1373

IN THE
Supreme Court of the United States

STATE OF UTAH,

Petitioner,

v.

EDWARD JOSEPH STRIEFF, JR.,

Respondent.

On Writ of Certiorari to the Supreme Court of Utah

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND TWENTY-ONE TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF RESPONDENT

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
CAITRIONA FITZGERALD
CLAIRE GARTLAND
AIMEE THOMSON
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. N.W.
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

January 29, 2016

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

CONSTITUTIONAL PROVISIONS

STATUTES

REGULATIONS

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C.[1] EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.

EPIC routinely participates as *amicus curiae* before this Court in cases concerning emerging privacy and civil liberties issues. *See, e.g.*, *Spokeo, Inc. v. Robins*, No. 13-1339 (filed Sept. 8, 2015) (arguing that the violation of a consumer's privacy rights under federal law constitutes an injury-in-fact sufficient to confer Article III standing); *City of Los Angeles, Cal. v. Patel*, 135 S. Ct. 2443 (2015) (arguing that hotel guest registries should not be made available for inspection absent judicial review); *Riley v. California*, 134 S. Ct. 2473 (2014) (arguing that the of search a cell phone incident to arrest requires a warrant); *United States v. Jones*, 132 S. Ct. 945 (2012) (arguing that a warrant is required for the use of GPS tracking techniques); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011) (arguing that the privacy interest in medical records justifies regulating datamining of prescription records); *Tolentino v. New York*, 562 U.S. 1043, (2010) (arguing that evidence

---

[1] Both parties consent to the filing of this brief. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

obtained from defendant's identity should be suppressed when discovered as a result of an unlawful stop), *dismissed as improvidently granted*, 563 U.S. 123 (2011); *Doe v. Reed*, 561 U.S. 186 (2010) (arguing that state law should not force the disclosure of petition signatories); *Herring v. United States*, 555 U.S. 135 (2009) (arguing for the suppression of evidence obtained as the result of an error in a criminal justice database); *Hiibel v. Sixth Judicial Dist. Ct. of Nevada*, *Humboldt Cty.,* 542 U.S. 177 (2004) (arguing that identification may not b compelled absent probable cause to arrest); *Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Stratton, Ohio*, 536 U.S. 150 (2002) (arguing that door-to-door petitioners should not have to obtain a permit and identify themselves).

Technical Experts and Legal Scholars

Alessandro Acquisti, Associate Professor, Information Technology and Public Policy, Carnegie Mellon University

Colin J. Bennett, Professor, University of Victoria

Dr. Whitfield Diffie, Visiting Scholar, Stanford, Center for International Security and Cooperation

Cynthia Dwork, Distinguished Scientist, Microsoft Research

Addison Fischer, Founder and Chairman, Fischer International Corp.

Hon. David Flaherty, former Information and Privacy Commissioner for British Columbia

Deborah Hurley, Institute for Qualitative Social Science, Harvard University

Ian Kerr, Canada Research Chair in Ethics, Law & Technology, University of Ottawa, Faculty of Law

Chris Larsen, CEO, Ripple, Inc.

Harry R. Lewis, Gordon McKay Professor of Computer Science, Harvard University

Dr. Pablo Garcia Molina, Adjunct Professor, Georgetown University

Peter G. Neumann, Senior Principal Scientist, SRI International

Helen Nissenbaum, Professor, Director of the Information Law Institute, New York University

Dr. Deborah Peel, M.D., Founder and Chair, Patient Privacy Rights

Chip Pitts, Chair, EPIC Board of Directors; Lecturer in Law, Stanford Law School

Bruce Schneier, Security Technologist; Author, Schneier on Security (2008)

Robert Ellis Smith, Publisher, Privacy Journal

Nadine Strossen, John Marshall Harlan II Professor of Law, New York Law School, Former President, American Civil Liberties Union

Frank Tuerkheimer, Professor of Law Emeritus, University of Wisconsin Law School

Sherry Turkle, Abby Rockefeller Mauzé Professor, MIT

Edward G. Vlitz, President and Chairman, Internet Collaboration Coalition

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

This case asks whether information available in the many thousands of government databases may provide *post hoc* justification for an unlawful detention. Recognizing the "digital Pandora's box" that such a practice would open, the answer must be "no."

A name is now no longer a simple identifier: it is the key to a vast, cross-referenced system of public and private databases that lay bare the most intimate features of an individual's life. If any person can be coerced by the state to hand over this key to the police, absent reasonable suspicion, then the protections of the Fourth Amendment have been rendered illusory.

Law enforcement databases now provide police officers with unprecedented access to details about the private lives of Americans. These databases contain not just outstanding warrants, but also personal financial and medical information, education records, property records, and Internet logs entirely unrelated to a criminal investigation. And much of the information in these databases is inaccurate, incomplete, and out of date.

Overturning the lower court decision in this case would permit compelled identification and the trolling of government databases, even after an unlawful detention. This goes far beyond what the Court permitted in *Hiibel* and *Terry*. As law enforcement databases continue to expand, there is an increased risk that the interest in accessing these databases will incentivize unlawful detentions.

ARGUMENT

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. As this Court has recognized, "[n]o right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law." *Terry v. Ohio*, 392 U.S. 1, 9 (1968) (internal quotation marks omitted).

Searches and seizures conducted without a warrant or probable cause are "*per se* unreasonable[,] subject only to a few specifically established and well-delineated exceptions." *City of Los Angeles, Cal. v. Patel*, 135 S. Ct. 2443, 2452 (2015) (internal quotation marks omitted). However, courts have recognized three tiers of police-citizen encounters that are permissible absent a warrant. *See* 4 Wayne R. LeFave, *Search and Seizure* § 9.4(e) (5th ed. 2012).

Tier one encounters involve consensual communications between an officer and citizen, which do not require probable cause or a warrant so long as the consent is voluntary and not "the product of duress or coercion, express or implied." *Schneckloth v. Bustamonte*, 412 U.S. 218, 227 (1973).

Tier three encounters rise to the level of arrest and are permitted if the officer has probable cause to believe that the individual has committed a crime in her presence, *Virginia v. Moore*, 553 U.S. 164, 178 (2008), or if she has probable cause to believe the person has committed a felony, *United States. v. Watson*, 423 U.S. 411, 421–23 (1976).

Tier two interactions, or "investigatory stops," occur when an officer briefly detains an individual without a warrant or probable cause. These stops are permissible only if the officer "has a reasonable, articulable suspicion that criminal activity is afoot." *Illinois v. Wardlow*, 528 U.S. 119, 123 (2000); *accord. Terry v. Ohio*, 392 U.S. 1, 21 (1968). The officer must be able to "point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion." *Terry*, 392 U.S. at 21.

Allowing information obtained from running an ID to attenuate the taint of unlawful activity will effectively eviscerate the requirement that investigatory stops be based on reasonable articulable suspicion. The growing size and scope of government databases means that running an ID will soon give the police access to information providing a *post hoc* justification for any police encounter, regardless of the initial level of suspicion.

I. Law enforcement agencies now have access to enormous databases of personal information that lack sufficient safeguards to ensure accuracy and reliability.

The accumulation of personal information stored in law enforcement databases is accelerating. There has been a dramatic increase in "the amount of digital information generated and stored about everyone." Comm. on Privacy in the Info. Age, Nat'l Research Council, *Engaging Privacy and Information Technology in the Digital Age* 272 (James Waldo et al. eds. 2007) [hereinafter "NRC *Engaging Privacy* Report"]. "Almost every activity in modern life, from

grocery shopping to surfing the Web to making a phone call, generates some record in a database somewhere." *Id*. at 271–72. Federal and state law enforcement agencies are increasingly gathering data to investigate crime and to make predictions about future crimes. Exec. Office of the President, *Big Data: Seizing Opportunities, Preserving Values* 29 (2014). Law enforcement officers have easy access to a broad array of information including criminal investigative records, travel and immigration records, and threat assessments. *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1, 10–14 (2008) (describing the rise in government data collection and risk profiling based on non-criminal conduct). Many of these systems were created to serve important law enforcement purposes, but their use over time has expanded and there are not sufficient protections to ensure that the data is accurate and reliable.

Law enforcement databases have grown increasingly complex over the last two decades. Risk scores are now assigned to individuals without any criminal past. Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score'*, Wash. Post (Jan. 10, 2016).[2] Local law enforcement surveillance "creates vast amounts of data, which is increasingly pooled in local, regional and national databases." *Id.*

---

[2] https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?hpid=hp_rhp-top-table-main_policesurvellance920p:homepage/story.

The development of criminal justice information systems in the United States has been ongoing for almost 50 years. In 1967, federal and local law enforcement agencies launched the National Crime Information Center ("NCIC"), a "nationwide information network operated by the Federal Bureau of Investigation" to provide access to "criminal justice information among federal, state, and local agencies." Office of Tech. Assessment, U.S. Congress, *A Preliminary Assessment of the National Crime Information Center and the Computerized Criminal History System* 3, 5 (1978) [hereinafter "1978 OTA Report"].

In the beginning, the NCIC contained only 356,784 records in five "file" categories. FBI, *National Crime Information Center*.[3] Ten years later, the database had integrated eight files including information from the Computer Criminal History system, which had more than 1,000,000 entries. 1978 OTA Report, *supra*, at 7. Today the NCIC has more than 13 million active records organized in 21 files. FBI, *National Criminal Information Center*, *supra*. States, cities, tribal agencies, sentencing commissions, penal institutions, railroad police departments, and private university police departments can now access the NCIC database. 28 U.S.C. § 534.

New systems have now been developed that enable law enforcement officers to search records from NCIC and other law enforcement databases

---

[3] https://www.fbi.gov/about-us/cjis/ncic (last visited Jan. 27, 2016).

directly from a mobile device. *See* Intellicheck, *Solutions Brief: Law Enforcement* (2015).[4] The FBI reports that during 2014 the NCIC "averaged 12 million transactions per day." FBI, *National Crime Information Center*, *supra*.

A. Law enforcement agencies are routinely collecting personal information about ordinary citizens.

Not everyone is a criminal or even a suspect, but everyone in the United States will eventually show up in one of the many databases maintained by federal and state law enforcement agencies. These records are no longer limited in geographic scope or subject matter—they are more than arrest and warrant records. Routine activities are subject to data gathering and analysis. And all of the data gathered is increasingly being compiled and analyzed in an attempt to flag suspicious patterns or behaviors.

1. FBI Databases

The FBI has recently created one of the largest collections of biometric identification data in the world, the Next Generation Identification ("NGI") system. Press Release, Criminal Justice Info. Servs. Div., FBI Announces Full Operational Capability of the Next Generation Identification System (Sept. 15,

---

[4] http://intellicheck.com/wp-content/uploads/2015/07/Law-ID-Solutions-Brief.pdf.

2014).[5] The NGI system was developed to expand the biometric identification capabilities of, and ultimately replace, the Integrated Automated Fingerprint Identification System, and to provide broader data collection capabilities. *Id*. As of December 2015, the NGI database contains more than 38 million civilian fingerprints (submitted for employment and licensing background checks) and more than 70 million criminal histories and fingerprints. FBI, *Next Generation Identification (NGI) Monthly Fact Sheet* (2015).[6] DOJ components and federal entities, as well as state, local, and tribal government entities, have direct access to these fingerprints. FBI, *Privacy Impact Assessment for Next Generation Identification (NGI) – Retention and Searching of Noncriminal Justice Fingerprint Submissions* (Feb. 20, 2015).[7]

In addition to fingerprints, the NGI database also stores iris scans, palm prints, and photographs of individuals. Criminal Justice Info. Servs. Div., FBI, *Next Generation Identification* 2 (2015).[8] The system includes facial recognition capabilities that analyze collected images, including over 23 million

---

[5] https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-full-operational-capability-of-the-next-generation-identification-system.

[6] https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/december-2015-ngi-fact-sheet.pdf.

[7] https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

[8] https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/ngi-one-pager-final.pdf.

front-facing photos currently stored in the database. *Id*. There were more than one million civilian photos, and nearly one million mugshot photos, added to NGI in 2015 alone. FBI, *Next Generation Identification (NGI) Monthly Fact Sheet*, *supra*.

In addition to the NGI and NCIC systems, the FBI also maintains a central repository of "information from local, state, regional, tribal, and federal criminal justice entities" called the National Data Exchange ("N-DEx"). FBI, *Privacy Impact Assessment for the National Data Exchange (N-DEx) System* (May 9, 2014) [hereinafter "FBI N-DEx PIA"].[9] The N-DEx database contains more than 500 million records, which are searched more than 315,000 times per month. Criminal Justice Info. Servs. Div., FBI, *Annual Report 2015*, at 11 (2015).[10]

The data in the N-DEx system includes personally identifiable information of "suspects, perpetrators, witnesses and victims, and anyone else who may be identified in a law enforcement report concerning a crime incident or criminal investigation." FBI N-DEx PIA, *supra*. Much of the information stored in N-DEx "is sensitive, and in the case of victim and witness information, it is highly sensitive." *Id*. The records in this database consist of incident, offense, and case reports, as well as arrest, booking, incarceration, and parole or probation

---

[9] https://www.fbi.gov/foia/privacy-impact-assessments/N-DEx.

[10] https://www.fbi.gov/about-us/cjis/annual-report-2015/2015_cjis_annual_report.pdf.

information from federal, state, local, and tribal law enforcement entities. *Id*. They include personal information such as an individual's name, sex, race, citizenship, date of birth, address, telephone number, Social Security Number, physical description, occupation, and vehicle information. *Id*. The FBI has acknowledged that increased disclosure of these records could pose significant privacy risks, but nevertheless the agency has provided automated access to its law enforcement partners. *Id.*

The FBI has sought to link its records even further by creating a Central Records System ("CRS"). Privacy Act of 1974; Notice of Modified Systems of Records, 63 Fed. Reg. 8659, 8671 (Feb. 20, 1998); *see also* Nat'l Archives, *FBI Central Records System*.[11] "Almost all FBI records are part of a case file in the CRS," Nat'l Archives, *supra*, and the CRS contains 281 categories of records. 63 Fed. Reg. at 8671. Individuals covered by CRS include individuals "who relate in any manner to official FBI investigations," including "subjects, suspects, victims, witnesses, and close relatives and associates who are relevant to an investigation." 63 Fed. Reg. at 8671. The CRS also includes records about "individuals who are the subject of unsolicited information, who offer unsolicited information, request assistance, and make inquiries concerning record material, including general correspondence, and contacts with other agencies, businesses, institutions, clubs; the public and the news media." *Id.* More recently the FBI has also moved to consolidate its warehoused records into

---

[11] https://www.archives.gov/research/investigations/fbi/central-records.html (last visited Jan. 26, 2016).

a centralized system, the FBI Data Warehouse. Privacy Act of 1974; System of Records, 77 Fed. Reg. 40,630, 40,631 (July 10, 2012); Privacy Act of 1974: Implementation, 77 Fed. Reg. 61,275, 61,275–76 (Oct. 9, 2012).

2. Fusion Centers

The Department of Justice and Department of Homeland Security are now making far more detailed personal information available to federal, state, and local law enforcement agencies than what was traditionally available in criminal justice records. Fusion centers, which operate at the local level, combine records from federal and state agencies, and government and private record systems. There are currently 78 fusion centers nationwide: 53 at the state level and 25 in major urban areas. DHS, *2014 National Network of Fusion Centers Final Report* 9 (Jan. 2015).[12] The fusion centers vary widely in size, funding, and operations. DOJ, *Fusion Center Guidelines* 3 (Aug. 2006) [hereinafter "Fusion Center Guidelines."].[13]

The term "fusion center" was first coined by the Department of Defense and refers to the fusing of information from different sources—public and private—for analysis purposes. *See* EPIC, *Information Fusion Centers and Privacy* (2016).[14] In

---

[12] http://www.dhs.gov/sites/default/files/publications/2014%20National%20Network%20of%20Fusion%20Centers%20Final%20Report_1.pdf.

[13] http://it.ojp.gov/documents/d/fusion_center_guidelines.pdf.

[14] https://www.epic.org/privacy/fusion/.

2002, the New York Times reported on the first fusion center project, managed by the Defense Advanced Research Project Agency. John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. Times (Nov. 9, 2002);[15] *see also*, William Safire, *You Are a Suspect*, N.Y. Times (Nov. 14, 2002).[16] Through the project, known as Total Information Awareness, the agency planned to "provide intelligence analysts and law enforcement officials with instant access to information from Internet mail and calling records to credit card and banking transactions and travel documents, without a search warrant." Markoff, *supra*.

Fusion centers began as the outgrowth of state-based intelligence analysis units, reviewing numerous streams of data from a variety of state-based sources. Todd Masse, Siobhan O'Neil & John Rollins, Cong. Research Serv., RL34070, *Fusion Centers: Issues and Options for Congress* 18–19 (July 6, 2007). Starting in 2006, the Department of Justice recommended that state fusion centers collect a broad range of data, including the personal information concerning individuals who are not suspected of any crime. Fusion Center Guidelines, *supra*, at 2.

The guidelines, subsequently developed by DHS and DOJ, continue to emphasize maximum information gathering and exchange involving "every

---

[15] http://www.nytimes.com/2002/11/09/politics/09COMP.html.

[16] http://www.nytimes.com/2002/11/14/opinion/you-are-a-suspect.html.

level and discipline of government, private sector entities, and the public." Fusion Center Guidelines, *supra*. Centers are encouraged to "fuse" a wide swath of data from government and private entities, including suspicious activity reports, fraudulent banking transactions, unemployment checks, firearm licenses, criminal histories, gang activity, credit reports, department of motor vehicle records, public health data, law enforcement investigation records, and probation, parole, and booking information from police and correctional institutions. *Id*. at Appendix C. States are now implementing programs that provide patrol cars with access to "fusion center" databases. G.W. Schultz, *Maryland to Store License-Plate Scanner Data at Intel Fusion Center*, Ctr. For Investigative Reporting (Aug. 9, 2010).[17]

The DOJ recommends that state fusion centers capture personal data about individuals by accessing a variety of government and commercial systems. Fusion Center Guidelines, *supra*, at 33–34. The DHS assists states in retrieving this information by identifying "key players" and intelligence requirements, facilitating information dissemination between different government agencies, and "provid[ing] security clearances to appropriate members of private sector leadership." *The Future of Fusion Centers: Potential Promise and Dangers: Hearings Before the Subcomm on Intelligence, Info. Sharing & Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 111th Cong. 16 (2010)

---

[17] http://www.centerforinvestigativereporting.org/blogpost/20100809marylandtostorelicenseplatescannerdataatintelfusioncenter.

(statement of Robert Riegle, Director, State and Local Program Office, Office of Intelligence and Analysis, DHS) [hereinafter "Riegle Fusion Center Statement"].

In 2010, the DHS established a new Federal Fusion Center and exempted all disclosures to state and local fusion centers from Federal Privacy Act obligations. Privacy Act of 1974: Department of Homeland Security Office of Operations Coordination and Planning–003 Operations Collection, Planning, Coordination, Reporting, Analysis, and Fusion System of Records, 75 Fed. Reg. 69,689 (Nov. 15, 2010). Going forward, DHS intends to establish a national fusion network. Riegle Fusion Center Statement, *supra*, at 35–36.

This increased data dissemination is problematic for many reasons, including the fact that fusion centers rely on information collected from government and commercial systems that can contain unreliable data. *See infra* Part I.B. Moreover, law enforcement personnel make use of these new integrated state databases even as states are suspending the privacy obligations and open government requirements that would otherwise require public accountability in the management of these systems. In the state of Virginia, for example, legislation was enacted that suspended the application of the Virginia Freedom of Information Act and the Virginia Collection and Dissemination Practices Act to the Virginia Fusion Center. H.B. 1007, 2008 Gen. Assem., Spec. Sess. (Va. 2008). *See* EPIC, *EPIC v. Virginia Department of State Police:*

Fusion Center Secrecy Bill (2016)[18] (revealing an MOU between the FBI and the Virginia State Police that required modifications in the state open records and privacy laws to permit the establishment of a fusion center in Virginia).

3. DHS Databases and Risk Profiling

Police also have access to programs that provide information not only about outstanding warrants, but also about speculative and secretive "scoring" of individuals. Fusion centers and other federal systems are increasingly providing local law enforcement officers with access to data collected by the DHS, the FBI, and other federal agencies as well as "watch lists" and other speculative risk profiles. *See* Info. Sharing Envt., *Law Enforcement Information Sharing* (describing the interconnection of state and local agencies with data from NCIC, N-DEx, and the DHS LEISS network).[19] The DHS also attempts to assign risk scores to individuals based on patterns, transit records, and other personal information.

Beginning in 2003, the Transportation Security Administration ("TSA") developed a program to collect and analyze data from a variety of sources in order to "prescreen" and "classify passengers according to their level of risk." U.S. Gov't Accountability Office, GAO-04-385, *Aviation Security: Computer-Assisted Passenger Prescreening Program Faces Significant Implementation Challenges* 2

---

[18] https://epic.org/privacy/virginia_fusion/.

[19] https://www.ise.gov/law-enforcement-information-sharing (last visited Jan. 28, 2016).

(2004) [hereinafter "GAO CAPPS Report"].[20] This program was intended to replace the Computer-Assisted Passenger Prescreening System ("CAPPS") that had been established by the Federal Aviation Administration and operated by airlines in the mid 1990s to identify and screen checked baggage that might contain dangerous material. *Staff Statement No. 3, The Aviation Security System and the 9/11 Attacks: Seventh Public Hearing of the Nat'l Comm'n on Terrorist Attacks Upon the U.S.* 6 (Jan. 2004).[21] The new system, first referred to as CAPPS II, would be operated by government agencies, rather than private companies, and would use experimental data-mining algorithms to assign risk scores to individual passengers and trigger special screening procedures. *See* EPIC, *Passenger Profiling* (2016).[22]

The initial launch of CAPPS II was plagued by errors, and the program was replaced by "Secure Flight." *See* TSA, TSA to Test New Passenger Pre-Screening Program (Aug. 26, 2004);[23] *see also* EPIC, *Secure Flight* (2016).[24] Under the program, the TSA collects passenger data—including the full name, date of birth, gender, redress number, known traveler number, and passport information—and itinerary data in order to assign risk scores. DHS, *Privacy*

---

[20] http://www.gao.gov/new.items/d04385.pdf.

[21] http://www.9-11commission.gov/staff_statements/staff_statement_3.pdf.

[22] https://epic.org/privacy/airtravel/profiling.html.

[23] https://web.archive.org/web/20060412081939/http://www.tsa.gov/public/display?theme=44&content=09000519800c6c77.

[24] https://epic.org/privacy/airtravel/secureflight.html.

Impact Assessment for the Secure Flight Program 4 (Aug. 9, 2007).[25] The TSA relies heavily on FBI "watchlists" that have been known to contain significant errors. *See* EPIC, *Documents Show Errors in TSA's "No Fly" and "Selectee" Watch Lists* (Mar. 26, 2006).[26]

The DHS has also created a similar "risk-based targeting" system within U.S. Customs and Border Patrol ("CBP") called the Automated Targeting System ("ATS"). The ATS "compares traveler, cargo, and conveyance information against intelligence and other enforcement data." DHS, *Automated Targeting System* 3 (Aug. 3, 2007).[27] The ATS system collects and correlates data from cargo shipments, passenger manifests, border crossing records, airline reservations, "nonimmigrant entry" records, and other information from law enforcement databases. *Id*. The TSA's Secure Flight database and the CBP's ATS database ostensibly draw from the same watchlists, though it took the DHS seven years to resolve "inconsistencies" between the two systems. DHS, *Privacy Impact Assessment Update for the Automated Targeting System—TSA/CBP Common Operating Procedure Phase II*, DHS/CBP/PIA-006(d) (Sept. 16, 2014) [hereinafter "ATS PIA 2014"].[28] The

---

[25] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight.pdf.

[26] https://epic.org/privacy/airtravel/foia/watchlist_foia_analysis.html.

[27] http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_ats_updated_fr_0.pdf.

[28] http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_tsacop_09162014.pdf.

ATS system also compares this data with "patterns" based on "officer experience, trend analysis of suspicious activity, law enforcement cases, and raw intelligence" to flag potential travelers who they feel might pose a risk. *Id*. at 1; *see also* EPIC, *Automated Targeting System* (2016).[29] The ATS system provides access to biographical information, itineraries, status, and other comments related to flagged individuals. ATS PIA 2014, *supra*, at 5.

In addition to the ATS system, CBP has developed another centralized system in an effort to identify "individuals, associations, or relationships that may pose a potential law enforcement or security risk." DHS, *Privacy Impact Assessment for the Analytical Framework for Intelligence (AFI)* 1 (June 1, 2012).[30] The primary function of AFI is to create an "index of relevant data in existing operational DHS source systems" and provide centralized access to that data based on personally identifiable information. *Id*. at 2. The AFI system also provides statistical, geospatial, temporal, and link analysis tools to review the centralized data about individuals. *Id*. at 4; *see also* EPIC, *EPIC v. CBP (Analytical Framework for Intelligence)* (2016).[31]

Local law enforcement agencies have also begun to develop their own risk profiling mechanisms. *E.g.*, Jouvenal, *supra*. For example, during a recent 911 call, the Fresno police

---

[29] https://epic.org/privacy/travel/ats/.

[30] http://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_afi_june_2012_0.pdf.

[31] https://epic.org/foia/dhs/cbp/afi/.

department used a private software program to calculate a man's "threat level" by scouring "billions of data points, including arrest reports, property records, commercial databases, deep Web searches and the man's social-media postings." *Id*.

The National Academy of Sciences has made clear that the risks of the growing complexity and scope of police databases "raise concerns about the privacy of those who are—rightly or wrongly—the targets of the new technologies." NRC *Engaging Privacy* Report, *supra*, at 254. "[T]he very fact that considerable amounts of data have been collected about individuals who have not been accused or convicted of a crime ensures that substantial amounts of information about non-criminals will end up in the databases of law enforcement agencies," even if agencies never look at or use the information. *Id.* at 253. But allowing records in databases to attenuate an unlawful police stop guarantees that this information *will* be used—used to give *post hoc* justification to evidence obtained through unlawful police activity.

B. Privacy Act exemptions and inaccurate data undermine the accuracy and reliability of determinations made by police.

Quantity, in the case of government databases, does not equal quality. Many of these databases are notorious for containing inaccurate and outdated information. The Department of Justice has made a bad problem worse by exempting its systems from key Privacy Act obligations, such as the requirement that records be accurate and timely, or that the public have an opportunity to correct the records. The

creation of criminal justice "risk scores" without transparency or scientific reliability will create a new set of problems. Overturning the decision below risks opening this "digital Pandora's box" of *post hoc* justifications for unlawful government detentions and seizures.

1. The federal government has exempted itself from maintaining accurate and timely records for many of its largest criminal justice databases.

The Department of Justice has led an effort to exempt government databases from the requirements that personal information stored by the federal government is accurate and reliable. It is inconceivable that the drafters of the Privacy Act would have permitted a federal agency to routinely collect and disseminate personal information without satisfying the accuracy and transparency requirements set out in the HEW Report. *See* U.S. Dep't of Health, Educ. & Welfare, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens* (1973).

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that federal agencies were able to collect. S. Rep. No. 93-1183, at 1 (1974). Congress further required agencies to be transparent in their information practices. *Id.*

In *Doe v. Chao*, 540 U.S. 614 (2004), the Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that "in order to

protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." *Doe*, 540 U.S. at 618.

But despite the clear pronouncement from this Court on accuracy and transparency in government records, the Department of Justice and Department of Homeland Security have exempted many of their law enforcement and risk assessment systems from key Privacy Act obligations. Specifically, the FBI and DHS claim exemptions from providing the following safeguards:

- Agencies must ensure that all records used to make determinations about an individual are accurate, relevant, timely and complete as reasonably necessary to maintain fairness. 5 U.S.C. § 552a(e)(5). The FBI and DHS have exempted all of the databases identified in Part 1.A from these accuracy and relevance requirements.[32]
- Agencies must allow individuals to access and review records contained about them in the database and to correct any mistakes. 5 U.S.C. § 552a(d). But the FBI and DHS have exempted all of the databases identified in

---

[32] *See* 28 C.F.R. § 16.96(g) (NCIC); 28 C.F.R. § 16.96(t) (N-Dex); 28 C.F.R. § 16.96(a) (CRS); 28 C.F.R. § 16.96(v) (FBI Data Warehouse); 49 C.F.R. § 1507.3(k) (Secure Flight); 28 C.F.R. § 16.96(r) (TSDB); 6 C.F.R. pt. 5, App. C 45 (ATS); 6 C.F.R. pt. 5, App. C 69 (AFI).

Part I.A from these access and correction requirements.[33]

- Agencies must collect and retain only such records "about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." 5 U.S.C. § 552a(e)(1). But the FBI and Department of Defense have exempted their databases identified in Section I.A from these relevance and necessity requirements.[34]
- Agencies must grant individuals access to an accounting of when, why, and to whom their records have been disclosed. 5 U.S.C. § 552a(c)(3). The FBI and DHS have opted not to provide access rights for individuals who have information in the databases identified in Part 1.A.[35]
- Agencies must publish notice of the database that discloses the sources of records contained in the database. 5 U.S.C. § 552a(e)(4)(I). The FBI and DHS refuse to disclose the categories of sources of records contained in the FBI Data

---

[33] *See supra* note 32.

[34] *See supra* note 32.

[35] *See supra* note 32.

Warehouse,[36] Secure Flight,[37] ATS,[38] and AFI.[39]

The Privacy Act is intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. But the FBI and DHS have effectively circumvented the intent of the Privacy Act while amassing large collections of personal information about ordinary citizens without adequate accountability.

This development should be of particular concern to the Court in this matter because police access to inaccurate and incomplete records across the federal government will expand dramatically if the decision of the lower court is overturned. In a case concerning police use of government databases, a diminished Fourth Amendment standard coupled with a weakened Privacy Act is truly a recipe for a loss of liberty in America.

2. Government databases are notorious for containing inaccurate and out-of-date records.

Many of these government databases are notoriously inaccurate. The Boston Police Department recently revealed that an internal database is "riddled with errors" that have affected "thousands of entries." Jordan Graham, *Boston Police to Update Traffic Stop Database*, Gov't Tech. (Jan. 20,

---

[36] 28 C.F.R. § 16.96(v).

[37] 49 C.F.R. § 1507.3(k).

[38] 6 C.F.R. pt. 5, App. C 45.

[39] 6 C.F.R. pt. 5, App. C 69.

2016).[40] The FBI's NGI biometric database has an error rate "as high as 20 percent." Timothy Williams, *Facial Recognition Software Moves From Overseas Wars to Local Police*, N.Y. Times (Aug. 12, 2015).[41] And a 2012 report by U.S. Senate Committee on Homeland Security and Governmental Affairs found that "fusion centers often produced irrelevant, useless or inappropriate intelligence reporting to DHS, and many produced no intelligence reporting whatsoever." Staff of Permanent Subcomm. on Investigations of the S. Comm. on Homeland Sec. and Governmental Affairs, 112th Cong., *Rep. on Federal Support for and Involvement in State and Local Fusion Centers* 2 (2012).[42]

FBI criminal records databases are also full of inaccuracies. All states provide arrest records to FBI databases such as NCIC and NGI.[43] But for the majority of states, less than 75 percent of these arrest records include final dispositions. U.S. Gov't

---

[40] http://www.govtech.com/public-safety/Boston-Police-to-Update-Traffic-Stop-Database.html.

[41] http://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html.

[42] *Available at* http://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04.

[43] For example, the Interstate Identification Index is a "cooperative federal- state program for the interstate exchange of criminal history record information for the purpose of facilitating the interstate exchange of such information among criminal justice agencies." Privacy Act of 1974; Notice of Modified Systems of Records, 64 Fed. Reg. 52,343, 52,344 (Sept. 28, 1999).

Accountability Office, GAO-15-162, *Criminal History Records, Additional Actions Could Enhance the Completeness of Records Used for Employment-Related Background Checks* 19 (2015) [hereinafter "GAO Criminal History Records Report"].[44] A 2013 report revealed that "1.8 million workers a year are subject to FBI background checks that include faulty or incomplete information," and that "50 percent of the FBI's [criminal] records fail to include information on the final disposition of the case." Madeline Neighly & Maurice Emsellem, *Wanted: Accurate FBI Background Checks for Employment*, Nat'l Emp't Law Ctr. 1 (July 2013).[45]

Government agencies also rely on private sector companies to compile information about citizens. *See, e.g.*, Fusion Center Guidelines, *supra*, at 33; LexisNexis Special Services Inc., *What We Do* (2015)[46] (stating that LNSSI "delivers a comprehensive suite of solutions to arm government agencies with superior data, technology and analytics to support mission success"). But private sector databases are known to be erroneous. *See, e.g.*, *Spokeo, Inc. v. Robins*, No. 13-1339 (U.S. argued Nov. 2, 2015) (concerning incorrect entries in a large public database containing profiles of consumers). The Government Accountability Office ("GAO") observed last year that "[p]rivate companies can face challenges in obtaining complete and accurate records, in part because not all states make their

---

[44] http://www.gao.gov/assets/670/668505.pdf.

[45] https://nelp.3cdn.net/bd23dee1b42cff073c_8im6va8d2.pdf.

[46] http://lexisnexisspecialservices.com/what-we-do/.

criminal record information accessible for private companies to search." GAO Criminal History Records Report, *supra*, at 37–38. In addition, the laws and regulations "that govern the gathering of information by the law enforcement establishment do not necessarily apply (or do not apply with clarity)" to private data aggregation companies, which amplifies the risk of inaccuracies. NRC *Engaging Privacy* Report, *supra*, at 275. Government use of private sector databases present the risk that law enforcement "will be able to avoid the restraints that have been placed on it to ensure the privacy of the individual citizen." *Id.*

"[M]isidentifications and erroneous watchlist entries" have also plagued the TSA and CBP databases. William J. Krouse, Cong. Research Serv., R42336, *Terrorist Watch List Screening and Background Checks for Firearms* 11 (2013).[47] For example, GAO reported in 2004 that the TSA's CAPPS II program faced "significant implementation challenges," in part because the TSA "has not yet determined the accuracy—or conversely, the error rate—of commercial and government databases that will be used by CAPPS II." GAO CAPPS Report, *supra*, at 14. Significant "false alerts" caused the TSA to abandon CAPPS II in favor of Secure Flight in 2004. TSA, *TSA to Test New Passenger Pre-Screening Program*, *supra*. The DHS then spent more than seven years attempting to resolve "inconsistencies" between the TSA's Secure Flight database and CBP's ATS database, which draw from the same FBI watchlists. *See* ATS PIA 2014, *supra*.

---

[47] https://www.fas.org/sgp/crs/terror/R42336.pdf.

The problems caused by erroneous and untimely data will only multiply as federal agencies look to increase interoperability without addressing accuracy. *See, e.g.*, *Interoperability Means Success for All Law Enforcement*, CJIS Link (FBI Washington, D.C.);[48] FBI, *Interoperability Initiatives Unit (IIU)*.[49] "[D]ata from different sources often arrives at different rates and with different data quality issues that can affect the ability to merge it together." Kalev Leetaru, *Policing Meets Big Data: A Lesson In Sentiment Mining, Data Recency And Dashboards*, Forbes (Jan. 17, 2016).[50] As huge data sets are shared between agencies at the federal, state, local, and tribal levels, inaccuracies will perpetuate and become harder to fully eliminate.

Because individuals do not have the ability to challenge erroneous entries in many of these databases, the consequences of incorrect entries go unchecked. For example, Jelani Henry spent two years in Riker's Island in pre-trial detention for a shooting he did not commit, including nine months in solitary confinement, before the charges were dismissed. Ben Popper, *How The NYPD Is Using*

---

[48] https://www.fbi.gov/about-us/cjis/cjis-link/may-2013/interoperability-means-success-for-all-law-enforcement (last visited Jan. 27, 2016).

[49] https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/iiubro4smallest-508-compliant.pdf (last visited Jan. 27, 2016).

[50] http://www.forbes.com/sites/kalevleetaru/2016/01/17/policing-meets-big-data-a-lesson-in-sentiment-mining-data-recency-and-dashboards/#469b93fc4acb.

Social Media to Put Harlem Teens Behind Bars, Verge (Dec. 10, 2014);[51] Meredith Broussard, *When Cops Check Facebook*, Atlantic (Apr. 19, 2015).[52] Henry was arrested because he had "liked" gang photos on Facebook. Broussard, *supra*; Popper, *supra*. As a result, he had been labeled as a gang affiliate in a law enforcement database—even though he was not involved and had only "liked" the photos to avoid social problems in his neighborhood. Broussard, *supra*.

Only one person—Rahinah Ibrahim—has succeeded in removing her name from the TSA's "No Fly" list. *Ibrahim v. DHS*, 62 F. Supp. 3d 909, 929 (N.D. Cal. 2014); Raymond Bonner, *"No-Fly List" Riddled with Errors, Impossible to Get Off of*, Informed Comment (Dec. 16, 2015).[53] In order to correct the error, Ibrahim went through ten years of litigation, including three appeals, before a trial revealed that Ibrahim had been improperly placed on a watchlist. 62 F. Supp. 3d at 929 ("Significantly, therefore, our case involves a conceded, proven, undeniable, and serious error by the government—not merely a risk of error."). Throughout the proceedings, the government steadfastly refused to confirm or deny any information about the list or their procedures. Bonner, *supra*.

---

[51] http://www.theverge.com/2014/12/10/7341077/nypd-harlem-crews-social-media-rikers-prison.

[52] http://www.theatlantic.com/politics/archive/2015/04/when-cops-check-facebook/390882/.

[53] http://www.juancole.com/2015/12/riddled-errors-impossible.html.

That so many databases containing sensitive personal information remain stricken with errors and inaccuracies cautions against relying on those databases to attenuate the taint of an unlawful police stop.

II. Overturning the decision below would permit suspicionless identification and defeat the protections established in *Hiibel* and *Terry*.

A. This Court has not permitted compelled identification absent reasonable articulable suspicion.

As this Court has previously held, officers can require individuals to identify themselves only during a stop based on reasonable suspicion. In *Hiibel v. Sixth Judicial Dist. Court of Nev., Humbolt Cty.*, this Court found constitutional a Nevada state law "requiring a suspect to disclose his name in the course of a valid *Terry* stop." 542 U.S. 177, 188 (2004). The Court noted first that "it is well established that an officer may ask a suspect to identify himself in the course of a *Terry* stop." *Id.* at 186. In condoning not just the ability to request identification but the ability to compel it with threat of criminal sanction, the Court concluded that the "request for identity has an immediate relation to the purpose, rationale, and practical demands of a *Terry* stop." *Id.* at 188.

In upholding an officer's ability to compel identification, however, the Court identified two critical limitations. First, the Nevada law only required Hiibel to "disclose his name." *Id.* at 185. The Court noted with approval that the statute did not require an individual to "give the officer a driver's

license or any other document," *id.*, or "'provide private details about his background,'" *id.* (quoting *Hiibel v. Sixth Judicial Dist.*, 59 P.3d 1201, 1206 (Nev. 2002) (opinion of Young, C.J.)). Second, compelled identification is permissible for the limited purposes of a *Terry* stop: An officer cannot compel identification "if the request for identification is not reasonably related to the circumstances justifying the stop." *Id.* at 188.

This Court has also recognized a number of important limitations on *Terry* stops. A *Terry* stop must not resemble a traditional arrest. *Dunaway v. New York*, 442 U.S. 200, 212 (1979). Instead, the scope of a *Terry* stop "must be carefully tailored to its underlying justification." *Florida v. Royer*, 460 U.S. 491, 500 (1983); *see Terry*, 392 U.S. at 19 (internal quotation marks omitted). A constitutionally reasonable *Terry* stop must be "justified at its inception" and "reasonably related in scope to the circumstances which justified the interference in the first place." *United States v. Sharpe*, 470 U.S. 675, 682 (1985). A *Terry* stop must also "be temporary and last no longer than is necessary to effectuate the purpose of the stop." *Royer*, 460 U.S. at, 500; *accord. United States v. Place*, 462 U.S. 696, 709–10 (1983).

During a *Terry* stop, the officer can also conduct a "reasonable search for weapons" only when the officer "has reason to believe that he is dealing with an armed and dangerous individual." *Terry*, 392 U.S. at 27. The "sole justification of the search" during a *Terry* stop "is the protection of the police officer and others nearby, and it must therefore be confined in scope to an intrusion reasonably designed to discover guns, knives, clubs, or other hidden instruments for the assault of the police officer." *Id.*

at 29. *See also Riley v. California*, 134 S. Ct. 2473, 2477 (2014) (outlining a similar rationale for searches incident to arrest).

But providing an officer with identification is no longer limited to the merely disclosing "a name." *Hiibel*, 542 U.S. at 185. Government databases now provide police officers with access to the exact private background details and other documents that the Nevada statute was supposed to prevent. *See id.* Information in government databases now extends far beyond whether a "suspect is wanted for another offense, or has a record of violence or mental disorder." *Id.* at 186.

The results of running an individual's identification are also no longer "reasonably related to the circumstances justifying the stop." *Hiibel*, 542 U.S. at 188. This Court defines a *Terry* stop as a limited intrusion that must be "justified at its inception" and "reasonably related in scope to *the circumstances which justified the interference in the first place*." *Sharpe*, 470 U.S. at 682 (emphasis added). But given the scope of information contained in government databases, an identification check quickly becomes an examination of databases containing sensitive personal information about the individual, including her potential involvement in, or "risk" of, committing other crimes.

B. Admitting the evidence in this case would create an end-run around the reasonable suspicion standards in Hiibel *and* Terry.

The lower court in this case rejected the argument that evidence obtained during an unlawful stop would nevertheless be admissible because the

officer compelled identification and discovered an unrelated warrant. *State v. Strieff*, 357 P.3d 532, 536 (Utah 2015). This Court should affirm that ruling because enforcing the prohibition on suspicionless identification is the only way to ensure that the Fourth Amendment protections outlined in *Hiibel* and *Terry* are upheld. Overturning the opinion would permit the results of an identification search to provide a *post hoc* justification for an unlawful detention. This would essentially create an end-run around the reasonable suspicion standard and enable routine identification of individuals in order to obtain evidence that would justify further escalation of the encounter.

This Court has recognized that "questions concerning a suspect's identity are a routine and accepted part of many Terry stops," but only to the extent justified and based on reasonable suspicion. *Hiibel*, 542 U.S. at 186, 188. Many states have explicitly recognized this requirement, passing laws that permit officers to identify a suspect only when they have reasonable suspicion. The states that have explicitly recognized this limitation include:

- Alabama. Ala. Code § 15-5-30 (2015) (reasonable suspicion);
- Arizona. Ariz. Rev. Stat. Ann. §§ 13-2412, 28-1595 (2015) (reasonable suspicion);
- Arkansas. Ark. Code Ann. § 5–71–213(a)(1) (2015) (Class C misdemeanor (loitering) to "linger[], remain[], or prowl[]" in a public place without apparent reason and, upon inquiry from law enforcement, refuse to provide identity);

- Colorado. Colo. Rev. Stat. § 16-3-103 (2015) (reasonable suspicion);
- Delaware. Del. Code Ann. tit. 11, §§ 1902(a) ("reasonable grounds"), 1321(6) (loitering) (2016);
- Florida. Fla. Stat. §§ 901.151 ("reasonably indicate that such person has committed, is committing, or is about to commit a violation of the criminal laws of [Florida] or the criminal ordinances of any municipality or county"), 856.021(2) (loitering) (2015);
- Georgia. Ga. Code Ann. § 16–11–36(b) (2015) (failure to identify oneself may be considered factor in determining whether individual is loitering);
- Illinois. 725 Ill. Comp. Stat. 5/107–14 (2015) ("[R]easonably infers from the circumstances that the person is committing, is about to commit or has committed an offense.");
- Indiana. Ind. Code § 34-28-5-3.5 (2014) (Class C misdemeanor to refuse to provide identity to a law enforcement officer who has stopped the person for an infraction or ordinance violation);
- Kansas. Kan. Stat. Ann. § 22–2402(1) (2015) (reasonable suspicion);
- Louisiana. La. Code Crim. Proc. Ann. art. 215.1(A) (2015) (reasonable suspicion);
- Missouri. Mo. Rev. Stat. § 84.710(2) (2015) (reasonable suspicion (Kansas City only));
- Montana. Mont. Code Ann. § 46–5–401(2)(a) (2015) ("particularized suspicion");
- Nebraska. Neb. Rev. Stat. § 29–829 (2015) (reasonable suspicion);

- Nevada. Nev. Rev. Stat. § 171.123 (2015) (reasonable suspicion);
- New Hampshire. N.H. Rev. Stat. Ann. §§ 594:2, 644:6 (Lexis 2015) (reasonable suspicion);
- New Mexico. N.M. Stat. Ann. § 30–22–3 (2015) (concealing identity with intent to obstruct the due execution of the law or hinder or interrupt any public officer is a petty misdemeanor);
- New York. N.Y. Crim. Proc. Law § 140.50(1) (McKinney 2015) (reasonable suspicion);
- North Dakota. N.D. Cent. Code § 29–29–21 (2015) (reasonable suspicion);
- Ohio. Ohio Rev. Code Ann. § 2921.29 (LexisNexis 2015) (reasonable suspicion);
- Rhode Island. R.I. Gen. Laws § 12–7–1 (2015) (reasonable suspicion);
- Utah. Utah Code Ann. § 77–7–15 (2015) (reasonable suspicion);
- Vermont. Vt. Stat. Ann. tit. 24, § 1983 (2015) (law enforcement officer may detain a person for refusing to identify themselves when requested by officer); and
- Wisconsin. Wis. Stat. § 968.24 (2015) (reasonable suspicion).

Overturning the lower court's opinion would permit law enforcement to circumvent these restrictions and routinely compel identification in order to search for information that would justify a seizure or arrest. There is now so much information available about ordinary citizens in government databases that routine ID checks could very well lead to prolonged detention or examination. *See* Part I.A,

supra. But much of the information in law enforcement databases is inaccurate or misleading, and the government has chosen to exempt its systems from the accuracy and transparency obligations established in the Privacy Act. *See* Part I.B., *supra*.

Furthermore, it would be inequitable to allow the results of an unlawful stop and identification to retroactively justify the improper behavior of the officer. This Court recently held that where an officer stops an individual based on a mistake about the applicable law or facts, that reasonable mistake does not retroactively render the stop unlawful. *See Heien v. North Carolina*, 135 S. Ct. 530, 536 (2014). But the government cannot have it both ways. If a reasonable mistake about the legal or factual predicate of a stop does not render that stop unlawful, then evidence discovered after an unlawful stop should not render the unlawfully seized evidence admissible. If data obtained during an identification search could retroactively change the lawfulness of a stop, then there would be a clear incentive to engage in suspicionless stops for identification purposes. Any ID check that linked an individual with data suggesting criminal intent would, in hindsight, justify the unlawful stop.

The widespread collection and dissemination of data about ordinary citizens requires even more vigilant protection of important Fourth Amendment interests. As Justice O'Connor recognized more than two decades ago:

> [T]he advent of powerful, computer-based recordkeeping systems [f]acilitate arrests in ways that have never before been possible. The police, of course, are entitled to enjoy the substantial

> advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.

Arizona v. Evans, 514 U.S. 1, 17–18 (1996) (O'Connor, J., concurring).

CONCLUSION

For the foregoing reasons, *amici* respectfully ask this Court to affirm the decision of the Supreme Court of Utah below.

Respectfully submitted,

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
CAITRIONA FITZGERALD
CLAIRE GARTLAND
AIMEE THOMSON
ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1718 Connecticut Ave. N.W.
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

January 29, 2016