No. 09-11556

IN THE

Supreme Court of the United States

JOSE TOLENTINO,

Petitioner,

v.

THE PEOPLE OF THE STATE OF NEW YORK,

Respondent.

On a Writ of Certiorari to
The New York Court of Appeals

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND LEGAL SCHOLARS AND TECHNICAL EXPERTS IN SUPPORT OF THE PETITIONER

MARC ROTENBERG
Counsel of Record
JOHN VERDI
ELECTRONIC PRIVACY
INFORMATION
CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140

January 19, 2011

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*[1]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. 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.[2]

EPIC has participated as *amicus curiae* in several cases before this Court and other courts concerning privacy issues, new technologies, and Constitutional interests. These cases include *Doe v. Reed*, 130 S. Ct. 2811 (2010); *Quon v. City of Ontario*, 130 S. Ct. 2619 (2010); *Flores-Figueroa v. United States*, 129 S. Ct. 1886 (2009); *Herring v. United States*, 129 S. Ct. 695 (2009); *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008); *Hiibel v. Sixth Judicial Circuit of Nevada*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Department of Justice v. City of Chicago*, 537 U.S. 1229 (2003); *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of*

---

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and the brief was not authored, in whole or in part, by counsel for a party.

[2] EPIC is grateful for the work of EPIC Fellows Conor Kennedy and Nichole Rustin-Paschal, who contributed to the preparation of this brief.

Stratton, 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000); and other federal and state cases.

EPIC has a particular interest in ensuring that individuals are able to maintain reasonable control over the disclosure of their identity, particularly when the release of this information enables access to a wide range of personal information stored across computer databases.

Technical Experts and Legal Scholars

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

Steven Aftergood, Senior Research Analyst, Federation of American Scientists

James Bamford, Author and Journalist

Grayson Barber, Esq. Grayson Barber, LLC

Christine L. Borgman, Professor and Presidential Chair in Information Studies, UCLA

Dr. David Flaherty, Former Information and Privacy Commissioner, British Columbia, Canada

Deborah Hurley, Consultant

Pradeep K. Khosla, Head, Department of Electrical and Computer Engineering, Carnegie Mellon University

Chris Larsen, CEO, Prosper

Pablo Molina, CIO, AVP of IT and Adjunct Professor, Georgetown University

Dr. Peter G. Neumann, Fellow of AAAS, ACM, IEEE, SRI International

Ray Ozzie, Chief Software Architect, Microsoft

Deborah C. Peel, MD, Founder and Chair, Patient Privacy Rights

Chip Pitts, Lecturer, Stanford Law School and Oxford University

Dr. Barbara Simons, IBM Research (retired)

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

In *Hiibel v. Sixth Judicial District,* 542 U.S. 177 (2004), this Court upheld a Nevada statute requiring individuals to state their name to a police officer because "the statute does not require a suspect to give the officer a driver's license or any other document." *Id.* at 186. This case presents the question, also in the context of a car stop with less than probable cause, whether a person should be required to present the driver's license. As the *Hiibel* minority noted, and the opinion for the Court did not dispute, a person's name is "the key to a broad array of information about the person, particularly in the hands of a police officer with access to a range of law enforcement databases." *Id.* at 196 (Stevens, J. dissenting). The risk is real that car stops will increasingly become pretextual because of the opportunity to search a government database for data unrelated to the reason that gave rise to the original stop.

Because of the circumstances of the stop in this case, the earlier decision of the Court in *Hiibel*, and *amici's* ongoing concern about the growing use of personal data by government without a clear law enforcement purpose, *amici* urge the Court to reverse the decision below.

ARGUMENT

I. A Traffic Stop Can Give Police Access to an Enormous Pool of Personal Data

Government databases give police officers access to an extraordinary range of detailed personal information. No longer does the stop of a vehicle provide access to simple information about the status of the car. Given a few minutes, police officers can search from their squad cars an increasingly sophisticated network of government data systems, and obtain personal information once scattered across municipal, state, and federal criminal databases that would never have been available in the context of a routine car stop. This capability underscores the need to safeguard drivers' privacy interests, particularly in view of the broad consensus that rapid technological change necessitates vigilant maintenance of cherished privacy safeguards. As one of the current Justices once wrote:

> [W]e sense a great threat to privacy in modern America; we all believe that privacy is too often sacrificed to other values; we all believe that the threat to privacy is steadily and rapidly mounting; we all believe that action must be taken on many fronts now to preserve privacy.

Samuel Alito, The Boundaries of Privacy in America 1 (1972) ("Report of the Chairman") (on file with *amici*).

A. Mobile Data Terminals

Government contractors offer products for police officers to capture biometric data from their patrol

cars and match it to state and federal databases. Standard products include iris scanners,[3] hand-held, mobile fingerprint scanners[4] and facial recognition cameras,[5] all enabling officers to record and search in near-real time. In Maricopa County, Arizona, a police unit specializing in biometric collection and "using a type of equipment prevalent in war zones, records 9,000 biometric digital mug shots a month." Dana Priest and William M. Arkin, *Monitoring America*, Wash. Post, Dec. 20, 2010, at 2.[6] These same devices are interoperable with both state and national criminal databases. *See, e.g.,* L-1 Identity

---

[3] *See* "Hiide Series 4," L-1 Solutions, http://www.l1id.com/pages/47-hiide-?rev=true.

[4] *See e.g.,* "IBIS Extreme," L-1 Identity Solutions, http://www.l1id.com/pages/536-ibis-extreme; Press Release, Datastrip, "Fairfax County Police Deploys Datastrip DSV2+TURBO Devices to Enhance Identification Accuracy in the Field," (Feb. 5, 2008) http://www.datastrip.com/press/Police_Deploys_Datastrip.html; "Positiveid+," Dynamic Imaging, http://www.dynamicimaging.com/positiveid/.

[5] *See e,g,* "FaceIt Argus" L-1 Identity Solutions, http://www.l1id.com/pages/71-facial-screening; Press Release, Datastrip, "Datastrip Adds Camera to DSVII Mobile Biometric ID Readers" (Sept. 25, 2006), http://www.datastrip.com/press/09.25.06%20Digital%20Still%20Camera.html; "Positiveid+," Dynamic Imaging, http://www.dynamicimaging.com/positiveid/.

[6] *Available at* http://projects.washingtonpost.com/top-secret-america/articles/monitoring-america/2/.

Solutions, *IBIS Extreme: How it Works*.[7] In such circumstances, the car stop provides an opportunity to gather further personal data about an individual regardless of whether any crime has occurred.

Officers can run fingerprint searches directly from their patrol car laptops and handhelds and conduct facial recognition searches with Blackberry, Android, or iPhone cellular phones. *See, e.g.,* Dynamic Imaging Systems, *PositiveID+ Facial Recognition & Fingerprint Identification: Mobile & Wireless Capabilities*.[8] Camera phones can be used to capture a subject's image and submit it to a matching server. *Id.* Within moments, personal data purportedly related to the individual is sent back on to the same device for retrieval and review. *Id.*

B. The National Crime Information Center

One of the largest repositories of personal information retrieved through mobile data terminals is the National Crime Information Center ("NCIC"). The NCIC is a searchable index of digital profiles. The FBI began the NCIC over fifty years ago to centralize the submission and retrieval of state criminal history records, or "rap sheets." *See Exploring Federal Solutions to the State and Local Fugitive Crisis*, *Hearing Before the S. Subcomm. On Crime and Drugs of the Comm. of the Judiciary*, 110th Cong. 2 (2010) (Statement of Roy G. Weise, Senior Advisor, Criminal Justice Information

---

[7] http://www.l1id.com/pages/533-ibis-extreme-how-it-works?rev=true.

[8] http://www.dynamicimaging.com/positiveid/features-benefits.aspx#mobile.

Services Division).[9] Since then, Congress expanded the system to include many new categories of sensitive data, including records of protection orders, missing or unidentified persons, and immigration violations. 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.

The NCIC operates over a private, national telecommunications network connecting squad cars across the country with state-based operators who have direct access to the NCIC index. Federal Bureau of Investigation, *National Crime Information Center*.[10] L-1's IntelliMobile "gives officers the ability to wirelessly access data and query the National Crime Information Center as well as local and state records simultaneously in real-time without having to radio dispatch." L-1 Identity Solutions, *L-1 Identity Solutions, Intellimobile – Solutions*.[11] The NCIC profiles accumulate more personal data as federal, state, and local law enforcement agencies voluntarily gather and submit personal information from convicted individuals, criminal suspects, and other persons of interest. *See id.* The NCIC is accessed up to 7.5 million times a day. *Id.*

Police across the country use NCIC profiles to track a large and diverse set of attributes. In Tennessee, Memphis city police officers "can use a

---

[9] Available at http://judiciary.senate.gov/pdf/11910%20Weise%20Testimony.pdf.

[10] http://www.fbi.gov/about-us/cjis/ncic/ncic.

[11] http://www.l1id.com/pages/425-intellimobile.

hand-held device to instantly call up a mug shot, a Social Security number, the status of the driver's license and any outstanding warrants," and an in-car laptop to learn "more about who owns the vehicle, the owner's name and address and criminal history, and who else with a criminal history might live at the same address." Dana Priest and William M. Arkin, *Monitoring America*, Wash. Post, Dec. 20, 2010, at 2.[12] NCIC profiles detail a subject's supervised release from prison, potential violations of immigration law, and status as a foreign fugitive, sex offender, wanted person, suspected terrorist, or gang member. Federal Bureau of Investigation, *National Crime Information Center*.[13] Court protection orders and Secret Service protective orders are recorded on NCIC profiles, in addition to registered instances of identity theft and missing or unidentified persons. *Id.*

The NCIC profiles consist of "fields" and "codes." *See generally,* Federal Bureau of Investigation, *NCIC Code Manual: Personal Descriptors,* Mar. 3, 2010 (available through the Oregon State Police Law Enforcement Data System website).[14] Each "field" is a space on an NCIC profile allocated for a particular item of personal information. *See id.* A "code" is an item of personal information corresponding to a field. *See id.* The NCIC provides a field for "Sex," which enables officers to enter the code "F" to signify that the subject of a profile is female. *Id.* at 7. When an

---

[12] http://projects.washingtonpost.com/top-secret-america/articles/monitoring-america/2/.

[13] http://www.FBI.gov

[14] http://www.oregon.gov/OSP/CJIS/NCIC.shtml.

officer submits an "F" in the "Sex" field of an individual's NCIC profile, every other agency who accesses that profile will know that the individual has been identified as female. There are thirty-four "personal descriptor" fields on NCIC profiles; each contains personal data about individuals. *Id.* at 2-4 ("Table of Contents"). Another field, "Offender Status," enables NCIC users to submit profile information pertaining to the subject's whereabouts (e.g., code "C4" signifies that the subject is "transient or homeless" and code "AY" signifies that the subject is known to be out of the country). *Id.* at 64-70.

The personal information transmitted by the NCIC is particularly invasive. Codes corresponding to the "SMT" field ("Scars, Marks, and Tattoos") provide submitters with abbreviated codes signaling that a subject has extra body parts (e.g., "EXTR BRST," "EXTR NIP"), missing body parts ("MISS BRSTS," "MISS PENIS," "MISS UTRUS"), implants ("ART BRSTS," "IMPL PENIS"), eating disorders ("MC EATDIS"), drug addictions ("DA GLUE"), past pregnancies ("MC PASTPRE"), and pierced body parts ("PRCD GNTLS"), among other sensitive attributes, such as non-abusive use of anti-depressants ("TD ADEPRES"). *Id.* at 17-40.

This is a vast array of personal data, available to a police officer in a patrol car, unrelated to motor vehicle safety or the enforcement of traffic laws.

C. The Integrated Automated Fingerprint Identification System

Another sizeable pool of retrievable sensitive data comes from the Integrated Automated Fingerprint Identification System ("IAFIS"): the largest biometric database in the world. Federal Bureau of Investigation, *Integrated Automated Fingerprint*

Identification System.[15] The IAFIS contains fingerprints from 66 million convicted and suspected criminals and 25 million "civil prints." *Id.* The FBI launched IAFIS in 1999, digitizing and streamlining the national repository of paper-based fingerprints it had maintained since 1924. *Id.* Fingerprint records in the IAFIS are accessible through the Interstate Identification Index ("III"), which police can access through the same network as the NCIC. Federal Bureau of Investigation, *Five Key Services*.[16]

In the wake of a decade of intelligence sharing initiatives, the IAFIS system is being formatted to accept fingerprint and digital photographs collected by Immigration and Customs Enforcement ("ICE")[17] and the Department of Homeland Security ("DHS")[18], enabling fingerprints submitted through one system

---

[15]http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis.

[16] http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_services; "National Crime Information Center," Mass.gov, http://www.mass.gov/?pageID=eopsterminal&L=3&L0=Home&L1=Law+Enforcement+%26+Criminal+Justice&L2=Criminal+Justice+Information+Services+%28CJIS%29&sid=Eeops&b=terminalcontent&f=chsb_cjis_ncic&csid=Eeops.

[17] ICE manages the United States Visitor and Immigration Status Indicator Technology ("US-VISIT").

[18] DHS manages the Automated Biometric Identification System ("IDENT").

to be checked against the others by default.[19] ICE plans to achieve full interoperability by 2013.[20]

As a consequence, police car stops will combine the identification techniques of biometrics with search across a wide range of government databases that contain individuals' personal, sensitive information.

D. E-Verify

The E-Verify program is a federal employment eligibility verification system ("EEVS") operated by the Department of Homeland Security ("DHS"). DHS, "E-Verify."[21] E-Verify is an Internet-based system that allows employers and others to submit an individual's personal information and receive a response stating the DHS's opinion concerning the individuals' citizenship status. *Id.* Experts and government reports have identified widespread inaccuracies in the E-Verify database.[22] The DHS

---

[19] Department of Homeland Security, *Privacy Impact Assessment for the Interim Data Sharing Model (iDSM) for the Automated Biometric Identification System (IDENT)/Integrated Autmated Fingerprint Identification System (IAFIS) Interoperability Project 2* (Sept. 1, 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_idsm.pdf; Press Release, U.S. Immigration and Customs Enforcement, *Secure Communities Strategy at Work in Fairfax County* (Mar. 16, 2010), http://www.ice.gov/news/releases/1003/100316fairfax.htm.

[20] Id.

[21] http://www.dhs.gov/files/programs/gc_1185221678150.shtm.

[22] Section II *infra*.

permits law enforcement agencies to access E-Verify data.[23] Police have arrested individuals based on E-Verify database queries.[24] In 2008, the state of Rhode Island mandated the use of E-Verify and directed State police officers to use the system as a basis for law enforcement initiatives.[25]

E. Fusion Centers

States are 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*.[26] Fusion centers began as the outgrowth of state-based intelligence analysis units, analyzing numerous streams of data from a variety of state-based sources. Todd Masse, Siobhan O'Neil & John Rollins, Cong. Research Serv., *Fusion Centers: Issues and Options for Congress, RL34070* 20, 19 (July 6, 2007). Starting

---

[23] Department of Homeland Security, *Privacy Impact Assessment for the E-Verify Program* at 34, May 4, 2010, www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_everify.pdf; *see also* 8 U.S.C. § 1357(g) (authorizing access to facilitate "performance of immigration officer functions by State officers and employees.").

[24] Philip Marcelo, *Impact of Carcieri's Immigration Order Under Scrutiny*, Providence Journal, Nov. 20, 2010.

[25] Gov. Donald L. Carcieri, Rhode Island Executive Order 08-01 (March 27, 2008); *but see* Gov. Lincoln Chafee, Rhode Island Executive Order 11-02 (January 5, 2011) (repealing E-Verify mandate).

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

in 2006, Federal Fusion Center Guidelines recommended that state fusion centers collect a wide stream of data, including substantial amounts of personal information concerning individuals who are not suspected of any crime. The guidelines direct fusion center to collect data regarding:

> Agriculture, Food, Water and the Environment, Banking and Finance, Chemical Industry and Hazardous Materials, Criminal Justice, Retail, Real Estate, Education, Emergency Services (Non-Law Enforcement), Energy, Government, Health and Public Health Services, Hospitality and Lodging, Information & Telecommunications, Military Facilities and Defense Industrial Base, Postal and Shipping, Private Security, Public Works, Social Services, [and] Transportation.

Global Justice Info. Sharing Initiative, Dep't of Justice, Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era -- Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels – Law Enforcement Intelligence, Public Safety and the Private Sector 2 (Aug. 2006). The Department of Justice recommends that state fusion centers capture personal data about individuals by accessing a variety of government and commercial systems, such as:

- Driver's license,
- Motor vehicle registration,
- Location information (411, addresses, and phone numbers),
- Law enforcement databases,

- National Crime Information Center (NCIC),
- NLETS -- The International Justice and Public Safety Information Sharing Network,
- the Terrorist Screening Center (TSC),
- Criminal justice agencies,
- Public and private sources (Security Industry databases, Identity Theft databases, Gaming Industry databases),
- Regional Information Sharing Systems
- (RISS)/Law Enforcement Online (LEO)
- U.S. Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN), including the United States Private-Public Partnership (USP3) – formerly HSINCI.
- Organizational and association resources
- InfraGard, The Infrastructure Security Partnership,
- Sex offender registries,
- Violent Criminal Apprehension Program (VICAP),
- Health- and Public Health-Related Databases (Public Health Information Network, Health Alert Network).

Id. at 33-34. The Department of Homeland Security 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 H.Comm on Intelligence, Info. Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Sec., 111th Cong. 16 (2010) (statement of Robert Riegle, Director, State and Local Program Office, Office of Intelligence and Analysis, Dept. of Homeland Sec.).

In 2010, the DHS proposed to establish a new Federal Fusion Center and exempt 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. 219, 69689 (Nov. 15, 2010). Going forward, DHS intends to establish a national fusion network. *The Future of Fusion Centers: Potential Promise and Dangers: Hearings Before the H.Comm on Intelligence, Info. Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 111th Cong. 35-36 (2010) (testimony of Robert Riegle, Director, State and Local Program Office, Office of Intelligence and Analysis, Dept. of Homeland Sec. and of Sheriff Leroy D. Baca, Los Angeles County Sheriff).

This increased data dissemination is problematic for many reasons, including the fact that fusion centers use erroneous information culled from government and commercial databases. Moreover, law enforcement personnel rely on 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 would suspend 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).

F. Combined DNA Index System

Statutes in all states require certain convicted offenders, including all felons, to submit DNA samples to be indexed in state-based DNA databases. National Conference of State Legislatures *DNA in Criminal Justice*[27] The collection of DNA is increasing and now includes many individuals who have not been convicted of any crime.

In 2008, state police officers in Daytona Beach, Florida deployed "special DNA kits" to collect DNA mouth swabs from persons of interest in a serial murder case. WKMG Orlando, *Police Swabbing Mouths During Traffic Stops in Serial Killer Hunt* (Feb. 6, 2008)[28] In 2009, the FBI decided to expand the collection of DNA samples at the federal level from convicts to all subjects of arrest. Solomon Moore, *F.B.I. and States Vastly Expand DNA Databases*, N.Y. Times, Apr. 18, 2009.[29] "The move, intended to help solve more crimes, is raising concerns about the privacy of petty offenders and people who are presumed innocent."[30] *Id.* One expert stated:

---

[27]http://www.ncsl.org/IssuesResearch/CivilandCriminalJustice/DNAinCriminalJustice/tabid/12727/Default.aspx.

[28] http://www.local6.com/news/15232197/detail.html.

[29]http://www.nytimes.com/2009/04/19/us/19DNA.html?_r=1.

[30] *Id.*

> "DNA databases were built initially to deal with violent sexual crimes and homicides — a very limited number of crimes," said Harry Levine, a professor of sociology at City University of New York who studies policing trends. "Over time more and more crimes of decreasing severity have been added to the database. Cops and prosecutors like it because it gives everybody more information and creates a new suspect pool."[31]

In 2010, California began taking DNA samples upon arrest, doubling the annual growth rate of its database to 390,000 profiles per year.[32] By 2012, the FBI expects its current database of 6.7 million profiles to expand by 1.2 million new profiles per year.[33]

II. Law Enforcement Officials Should Not Routinely Rely on Inaccurate Identity-Based Information Systems

Increasingly, law enforcement officials and other government employees are relying on government and commercial databases full of mistakes that are well-documented but rarely corrected. Government systems include the NCIC database and databases associated with the federal government's employment E-Verify system. Commercial databases include information from databrokers such as Choicepoint. As these errors are distributed to various law

---

[31] *Id.* (Harry Levine, a professor of sociology at City University of New York).

[32] *Id.*

[33] *Id.*

enforcement and other groups through the Information Sharing Environment and fusion centers, enormous difficulties are created for innocent individuals.

A. Inaccuracies in the National Crime Information Center ("NCIC")

The NCIC, discussed in Section I above, is a system that makes criminal history information widely available to police officers and law enforcement officials across the United States. FBI, *National Crime Information Center*.[34]

The problem of record accuracy has plagued the NCIC system for years. According to the Bureau of Justice Statistics ("BJS"), "[i]n the view of most experts, inadequacies in the accuracy and completeness of criminal history records is *the single most serious deficiency* affecting the Nation's criminal history record information systems." Bureau of Justice Statistics, *Use and Management of Criminal History Record Information: A Comprehensive Report*, 2001 Update, NCJ 187670 at 38 (Dec. 2001) (emphasis added).

In the most recent report, the BJS detailed ongoing concerns about errors in NCIC databases. BJS, *Improving Access to and Integrity of Criminal History Records*, NCJ 200581 (July 2005). The BJS points to problems with State criminal history records, which are fed into the NCIC. "Recent BJS surveys have suggested that criminal history repositories are encountering several problems

---

[34] http://www.fbi.gov/about-us/cjis/ncic/ncic.

including significant backlogs, older records that have no dispositions, and infrequent audits to ensure accuracy of records." *Id.* Also, "Repositories in States that could estimate the size of their backlogs in 2001 reported that 2.5 million records of arrest, disposition, and custody information were unprocessed or only partially processed." *Id.*

Though the errors are well-known, the BJS found that audits of these records are infrequent. "In 2001, 23 State criminal history repository directors reported that their databases had not been audited for completeness in the prior 5 years. [...] Over half of those States (13) reported that they had not planned or scheduled a data quality audit to occur within the next 3 years. Overall, 24 States did not plan to perform a data quality audit within 3 years of the survey." *Id.*

The BJS said in 2001 that, if incomplete or inaccurate records are used *"there is a substantial risk that the user will make an incorrect or misguided decision*." *Id.* (emphasis added*)*. Because the criminal history information is available to both private and public entities, misguided decisions may lead to an unjustified arrest, a lost employment opportunity, or inability to purchase a firearm. *Id.* There have not been many "in-depth audits or reviews of the accuracy of the information maintained by State and Federal criminal history record repositories" conducted, according to the report, but "most of those that have been conducted have found unacceptable levels of inaccuracies." *Id.* at 39.

The Department of Justice has sought to address concerns about record accuracy through the National Criminal History Improvement Program ("NCHIP").

Dep't of Justice, Bureau of Justice Statistics, *National Criminal History Improvement Program (NCHIP)*.[35] The goal of the program is to "insure that accurate records are available for use in law enforcement," and to provide "direct funding and technical assistance to the States to improve the quality, timeliness and immediate accessibility of criminal history and related records." *Id.* Between 1995 and 2002, more than $390 million dollars were allocated under the NCHIP program. Bureau of Justice Statistics, *Improving Criminal History Records for Background Checks* (May 2003).[36]

Nonetheless, as the 2005 BJS report makes clear, record accuracy continues to plague the criminal justice system. And with the continued expansion of the NCIC and the growth of fusion centers, the problem will become more severe.

Even though the federal Privacy Act makes clear the need to ensure accurate records and the federal government recognizes that these databases are filled with errors, that has not stopped federal agencies from increasingly attempting to exempt themselves from Privacy Act of 1974, 5 U.S.C. § 552a, provisions that require record accuracy. The agencies attempt to exempt themselves under §552a(j) (general exemptions) and §552a(k) (specific exemptions). 5 U.S.C. §§ 552a(j), (k). Such exemptions from the general accuracy requirements applicable to government record-keeping systems undermine the argument that there are alternatives to the

---

[35] http://www.ojp.usdoj.gov/bjs/nchip.htm.

[36] http://www.ojp.gov/bjs/abstract/ichrbc.htm.

exclusionary rule that will produce the appropriate level of accuracy.

The NCIC is an important and widely used database that is full of record inaccuracies. Yet, in 2003, the Department of Justice chose to exempt the NCIC from numerous mandates established by the Privacy Act, 5 U.S.C. § 552a, most notably accuracy requirements. As a result of this exemption, the FBI need not comply with 5 U.S.C. § 552a(e)(5), which requires an agency to "maintain all records which are used by the agency in making any determination about an individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual[.]" 5 U.S.C. § 552a(e)(5). The NCIC is also exempt from 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 § 552(e)(1).

B. Problems with Databases Associated with the Federal Government's Employment Eligibility Verification System

As discussed in Section I *supra*, law enforcement agents have access to E-Verify, the federal government's current employment eligibility verification system ("EEVS"). Several reports highlight inaccuracies in the government database used for employment verification. The errors in the federal government's employment eligibility verification system are so egregious and their effects so significant, that a federal judge cited to them in an opinion granting a temporary restraining order against the Department of Homeland Security.

The government reports documenting the errors in databases connected with EEVS date back more than 10 years. In a 1997 report and a 2002 follow- up review, the Inspector General of the Department of Justice found that data from the Immigration and Naturalization Service (the predecessor of U.S. Citizenship and Immigration Services) were unreliable and "seriously flawed in content and accuracy." Office of Inspector Gen., Dep't of Justice, *Immigration and Naturalization Service Monitoring of Nonimmigrant Overstays*, Rept. No. I-97-08 (Sept. 1997); *Follow-Up Report on INS Efforts to Improve the Control of Nonimmigrant Overstays*, Rept. No. I-2002-006 (Apr. 2002); and *Immigration and Naturalization Service's Ability to Provide Timely and Accurate Alien Information to the Social Security Administration*, Rept. No. I-2003-001 (Nov. 2002).

In August 2005, the Government Accountability Office investigated and found myriad errors in information from DHS databases searched through its employment eligibility verification system. Gov't Accountability Office, *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts*, GAO-05-813 25 (Aug. 2005).

The Social Security Administration's Office of Inspector General found accuracy problems in databases of Citizenship and Immigration Services and Social Security Administration. Office of Inspector Gen., Soc. Sec. Admin, *Congressional Response Report: Accuracy of the Social Security Administration's NUMIDENT File*, A-08-06-26100 (Dec. 18, 2006). The Inspector General estimated that about 17.8 million records in the Social Security Administration's Numerical Identification File

("NUMIDENT") have discrepancies with name, date of birth or death, or citizenship status. *Id.* at 6. About 13 million of these incorrect records belong to U.S. citizens, he said. *Id.* at Appendix C-2.

A federal judge pointed to the problems in NUMIDENT in an October 2007 opinion granting a temporary restraining order enjoining the Department of Homeland Security from implementing a new "no-match" employment eligibility verification proposal.

> As demonstrated by plaintiffs, the government's proposal to disseminate no-match letters affecting more than eight million workers will, under the mandated time line, result in the termination of employment to lawfully employed workers. This is so because, as the government recognizes, the no-match letters are based on SSA records that include numerous errors.

AFL-CIO v. Chertoff, 552 F. Supp. 2d 999 (N.D. Cal. 2007).

It is clear that the federal government's employment eligibility verification system is based on erroneous databases. As fusion centers continue to mix and mingle data from a multitude of government and commercial databases without clear accuracy or relevance obligations, the risk of record inaccuracy and data misuse increases. This strongly implicates the accuracy and reliability of the criminal justice records that would become accessible from a patrol car.

Multiple government assessments state that the watch lists remain filled with errors. The Justice Department Inspector General has said this indicates "a deficiency in the integrity of watchlist

information."[37] These watch lists are used to screen "approximately 270 million individuals . . . each month."[38] Such mistakes show it is paramount that government entities are held accountable for accuracy of their databases.

C. Commercial Databases on Which Law Enforcement Rely Are Also Inaccurate and Incomplete

There is extensive documentation of errors in commercial databases, as well. The government has increasingly relied upon these databases in its law enforcement activities and, as explained earlier, the federal Fusion Center Guidelines urge the intermingling of commercial data with information culled from government systems. For example, databroker Choicepoint trumpets on its Web site the various federal, state, local and law enforcement "solutions" that the company offers. These reports often include information that is erroneous, out of date, incomplete, unreliable, or just flat-out false.

A man bought his Choicepoint record and found that the file showed he had died in 1976. Jane Black, *Data Collectors Need Surveillance, Too,* Business Week, Jan. 24, 2002. Another man's report included numerous crimes that he never committed. "In Florida I'm a female prostitute (named Ronnie); in Texas I'm currently incarcerated for manslaughter," according to the man. Kim Zetter, *Bad Data Fouls Background Checks*, Wired News, Mar. 11, 2005.

---

[37] Justice Dept. Report on Watch Lists at xxii.

[38] *Id.* at v.

Also, "in New Mexico I'm a dealer of stolen goods. Oregon has me as a witness tamperer. And in Nevada – this is my favorite – I'm a registered sex offender."[39]

Another Choicepoint file contained significant errors. The record of one woman listed "possible Texas criminal history" even though she has been to Texas only twice and has not been charged with or committed crimes there. Bob Sullivan, *ChoicePoint Files Found Riddled With Errors*, MSNBC, Mar. 8, 2005. Her record also included "three automobiles she never owned and three companies listed that she never owned or worked for."[40]

When a news reporter looked up his file on databroker Intellius.com, he found the record said he was charged with child molestation (he wasn't) and that he had a close male relative who was convicted of manslaughter (the reporter had never even heard of the man). Bob Sullivan, *Red Tape Chronicles: Bob the Writer, Bob the Molester*, MSNBC, May 3, 2006.

These are just a few of the many erroneous records that have been compiled by Choicepoint and other databrokers used by the federal government for law enforcement purposes.

---

[39] *Id.*

[40] *Id.*

III. Driver Identity Information Is Entitled to Strong Privacy Protection

A. The Drivers Privacy Protection Act

In *Reno v. Condon*, 528 U.S. 141 (2000), the Supreme Court upheld the 1994 Drivers Privacy Protection Act ("DPPA"), which protects the personal information contained in DMV record systems maintained by the states. 18 U.S.C. § 2721 ("Prohibition on release and use of certain personal information from State motor vehicle records.") The DPPA "generally prohibits any state DMV, or officer, employee, or contractor thereof, from 'knowingly disclosing or otherwise making available to any person or entity personal information about any individual obtained by the department in connection with a motor vehicle record.' 18 U.S.C. § 2721(a)." *Reno v. Condon,* 528 U.S. at 144. The DPPA reflects a determination by Congress that even though individuals may be required to provide certain personal information to obtain a driver's license, that information should be protected and should be disclosed and used only for appropriate purposes.

Under the DPPA, the disclosure of "personal information" is restricted. "Personal information" is defined as "names, photographs, social security numbers, drivers license numbers, addresses, telephone numbers, and medical and disability information of individuals." 18 U.S.C. § 2725(3). The statute sets out limited circumstances when personal information may be disclosed and provides penalties for violations of the Act. 18 U.S.C. § 18 U.S.C. 2721(b) ("Permissible uses.") "The DPPA's ban on disclosure of personal information does not apply if drivers have consented to the release of their data," *Reno v.*

Condon, 528 U.S. at 144, however such consent does not exist where a driver is required to provide their license to a police officer in the context of a car stop.

In *Reno*, a unanimous Court held the DPPA to be a proper exercise of Congress' regulation of interstate commerce and does not abridge federalism principles. Chief Justice Rehnquist found that the "DPPA regulates the States as the owners of databases . . . . The DPPA regulates the universe of entities that participate as suppliers to the market for motor vehicle information-the States as initial suppliers of the information in interstate commerce and private resellers or redisclosers of that information in commerce." *Id.* at 151. The Court also found that "The DPPA regulates the disclosure and resale of personal information contained in the records of state DMV's by limiting the state's ability to disclose a driver's personal information without her consent." *Id.* at 143-44.

In *Reno*, *amici* EPIC urged the Court to hold that the DPPA "is a valid exercise of federal authority in that it seeks to protect a fundamental privacy interest." Brief of Amicus Curiae Electronic Privacy Information Center at 1, *Reno v. Condon*, 528 U.S. 141 (2000). EPIC observed that "The states should not impermissibly burden the right to travel by first compelling the collection of sensitive personal information and then subsequently disclosing the same information for unrelated purposes." *Id.* at 1.

B. Application of Reno

Following *Reno*, federal and state courts have applied the decision in other cases involving the disclosure of personal information contained in DMV records. While a federal trial court found in *Russell v.*

Choicepoint, 302 F. Supp. 2d 654 (E.D. La. 2004), that *Reno* did not make any determinations about the scope of the statute when it held that the privacy protections in DPPA were constitutional, the Supreme Court of Iowa explained that Congress' intent to limit access to personal information in state motor vehicles databases means that "disclosure essentially depends on the use sought for the information, and the states are charged with the responsibility to ensure that disclosure is limited to those circumstances where Congress determined that the use for the information trumps the competing privacy interest." *Locate.Plus.Com, Inc. v. Iowa Dept. of Transp.*, 650 N.W.2d 609, 616 (Iowa 2002); *see also O'Brien v. Quad Six, Inc.*, 219 F.Supp.2d 933, 934-935 (N.D. Ill. 2002) (finding that the DPPA "seeks to control dissemination of information collected using the coercive power of the state.").

Courts routinely emphasize *Reno*'s interpretation of the DPPA as highly protective of drivers' personal information. *DeVere v. Attorney General,* 146 N.H. 762, 768 (N.H. 2001), construed New Hampshire's amended DPPA to mean that "in light of" the New Hampshire "statute's general prohibition against disclosure, this procedure [allowing in certain circumstances a court ordered disclosure of DMV records for the benefit of a private party . . . cannot be read to provide a general right of access to private parties simply by invoking the court's status as a governmental agency." *Id. See also*, *Myerson v. Prime Realty Services, LLC* 796 N.Y.S.2d 848 (2005) (explaining that "[t]here is a broad federal policy against the government revealing individuals' social security numbers. There are a variety of federal statutory restrictions on dissemination of such

information, such as the federal Driver's Privacy Protection Act of 1994").

Courts have also found that the other state agencies receiving funds subject to the terms of DPPA are expected to protect personal information even if they are not themselves departments of motor vehicles. *See*, *Hartman v. Dept. of Conservation and Natural Resources*, 892 A.2d 897, 901-902 (Pa. Commw. 2006), determining that state agencies made subject to the DPPA by another federal statute, such as the Transportation Equity Act for the 21st Century (TEA-21, Pub.L. No. 106-69, 113 Stat. 986, 1025-1026 (1999), "makes any recipient of the transportation funds subject to the terms of the DPPA, regardless of whether that person is a "State Department of motor vehicles."

In terms of permissible uses, courts have determined that the "DPPA affords states discretion to disburse DMV records for a permissible purpose under the statute," *Taylor v. Acxiom Corp.*, 612 F.3d 325 (5th Cir. 2010). In *Young v. West Pub. Corp.*, 724 F.Supp.2d 1268, 1279 (S.D. Fl. 2010), the District Court found that while the DPPA does not apply if drivers have consented to the release of their data, the DPPA "was intended to prevent unfettered access to personal information and to give individuals more control over the disclosure of their personal information, while continuing to allow state departments of motor vehicles to disclose the information for legitimate government and business needs." *Graczyk v. West Pub. Corp.,* 2009 WL 5210846, at *5 (N.D. Ill. 2009). Furthermore, "[t]he DPPA is written to restrict uses of personal information rather than users of that information." *Id.* at *4.

A private right of action has been upheld by courts applying *Reno* in other cases involving the DPPA. In *McCready v. White*, 417 F.3d 700, 703 (7th Cir. 2005), the Seventh Circuit found that the DPPA "authorizes private suits, but only by persons whose information has been disclosed improperly." In *Collier v. Dickinson*, 477 F.3d 1306 (11th Cir. 2007), the Eleventh Circuit found that the statutory right to privacy created by DPPA was enforceable separately under Section 1983 and that officials were not entitled to qualified immunity. "We find that the plain language of the DPPA clearly, unambiguously, and expressly creates a statutory right which may be enforced by enabling aggrieved individuals to sue persons who disclose their personal information in violation of the DPPA."477 F.3d at 1309-10.

CONCLUSION

Amici respectfully ask this Court to grant Petitioner's motion and reverse the decision of the lower court.

Respectfully submitted,

MARC ROTENBERG
JOHN VERDI
ELECTRONIC PRIVACY
INFORMATION
CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
p: (202) 483-1140
f: (202) 483-1248
email: rotenberg@epic.org

January 19, 2011