No. 12-25

IN THE

Supreme Court of the United States

EDWARD F. MARACICH, ET AL.,

Petitioners,

v.

MICHAEL EUGENE SPEARS, ET AL.,

Respondents.

**On Writ of Certiorari to
The United States Court of Appeals
For the Fourth Circuit**

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

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

November 16, 2012

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

ADMINISTRATIVE & LEGISLATIVE MATERIALS

OTHER AUTHORITIES

REGULATIONS

INTEREST OF THE *AMICI CURIAE*

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.[1]

EPIC routinely participates as *amicus curiae* before this Court and other courts in cases concerning federal privacy statutes: *FAA v. Cooper*, 132 S. Ct. 1441 (2012); *First Am. Fin. Corp. v. Edwards*, 610 F.3d 514 (9th Cir. 2010), *cert. denied as improvidently granted*, 132 S. Ct. 2536 (2012); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011); *NASA V. Nelson*, 131 S. Ct. 746 (2011); *Flores-Figueroa v. United States*, 556 U.S. 646 (2009); *Doe v. Chao*, 540 U.S. 614 (2003); *Gordon v. Softech Int'l, Inc.*, No. 10-5162, 2011 WL 1795300, *appeal docketed*, No. 12-0661 (2nd Cir. 2012); *In re Google Inc. St. View Commn'cs*, 794 F. Supp. 2d 1067 (N.D. Cal. 2011), *appeal docketed*, *Ben Joffe v. Google*, No. 11-17483 (9th Cir. Oct. 17, 2011); *Ostergren v. Cuccinelli*, 615 F.3d 263 (4th Cir. 2010); *SEC v. Rajaratnam*, 622 F.3d 159 (2nd Cir. 2010); *NCTA v. FCC*, 555 F.3d 996

---

[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 this brief was not authored, in whole or in part, by counsel for a party. EPIC Appellate Advocacy Fellow David Brody contributed to this brief.

(D.C. Cir. 2009); *Am. Bankers Ass'n v. Gould*, 412 F.3d 1081 (9th Cir. 2005); *United States v. Councilman*, 418 F.3d 67 (5th Cir. 2005); *Kehoe v. Fidelity Bank & Trust*, 421 F.3d 1209 (7th Cir. 2005).

EPIC has a particular interest in ensuring the effective enforcement of federal statutes that seek to protect the privacy of personal information. EPIC submitted an *amicus* brief in *Reno v. Condon*, 528 U.S. 141 (2000), in which we argued that "[t]he Drivers Privacy Protection Act safeguards the personal information of licensed drivers from improper use or disclosure. It is a valid exercise of federal authority in that it seeks to protect a fundamental privacy interest."

The EPIC amicus brief is joined by twenty-seven technical experts and legal scholars.

Technical Experts and Legal Scholars

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

Grayson Barber, Esq., Grayson Barber, LLC

Ann Bartow, Professor of Law, Pace Law School

Colin J. Bennett, Professor, University of Victoria

Francesca Bignami, Professor, George Washington University School of Law

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

Dr, danah boyd, Senior Researcher, Microsoft Research

Simon Davies, Project Director, London School of Economics

Dr. Cynthia Dwork, Researcher, Microsoft

Dr. Addison Fischer, Former Owner, RSA Data Security, Co-Founder, Verisign

Hon. David H. Flaherty, Professor Emeritus of History and Law, University of Western Ontario; Information Privacy Commissioner for British Columbia, 1993-99

Deborah Hurley, Chair, EPIC Board of Directors

Pamela S. Karlan, Professor, Stanford Law School

Jerry Kang, Professor of Law, UCLA School of Law

Ian Kerr, Associate Professor, Canada Chair of Ethics, Law, and Technology, University of Ottawa

Chris Larsen, CEO, Ripple

Gary T. Marx, Professor Emeritus of Sociology, MIT

Mary Minow, Library Law Consultant

Pablo Molina, Adjunct Professor, Georgetown University

Dr. Peter G. Neumann, SRI International

Helen Nissenbaum, Professor, Media, Culture & Communication, NYU

Frank A. Pasquale, Schering-Plough Professor in Health Care Regulation and Enforcement, Seton Hall Law School

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

Ronald L. Rivest, Professor of Electrical Engineering and Computer Science, MIT

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

Dr. Barbara Simons, (former) IBM Research

Edward G. Viltz, www.InternetCC.org

(Affiliations are for identification only)

SUMMARY OF THE ARGUMENT

The Driver's Privacy Protection Act of 1994 ("DPPA") protects the privacy of personal information. The Act prohibits the disclosure, except in narrow circumstances, of the information individuals are required by law to provide in order to obtain identification documents, drivers licenses, and

automobile titles. The improper release and misuse of this information creates a significant risk of harm to individuals.

The amount of personal information, including authenticating documents used to establish identity, obtained by state departments of motor vehicles ("DMVs") is staggering and has increased over time. The Department of Homeland Security ("DHS") now requires DMVs to collect and store detailed personal information, sensitive identifying documents, and biometric data. The records also contain Social Security numbers ("SSNs"), which are the key to identity theft, a top concern of American consumers.

The DPPA provides for disclosure of motor vehicle records for certain limited purposes. An expansive reading of any of those exceptions, including the "litigation" exception, would be inconsistent with the Act's goal of protecting personal information. Changes in technology have increased the risk of the underlying harm that Congress sought to address. Therefore, the Court should narrowly construe the statutory exceptions.

ARGUMENT

The Driver's Privacy Protection Act of 1994 ("DPPA"), 18 U.S.C. §§ 2721-2725, was enacted to protect individuals from the harm caused by misuse and unauthorized disclosure of the personal information they provide to state agencies that maintain motor vehicle records. The DPPA protects Americans from both physical[2] and financial[3] harms. In addition, the DPPA provides important limits on the collection and use of personal information by data brokers. *See* Sasha Romanosky & Alessandro Acquisti, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 Berkeley Tech. L. J. 1061, 1061 (2009).

At issue in this case is the interpretation of a particular exception in the Act. 18 U.S.C. § 2721(b)(4).[4] *Amici* EPIC, technical experts, and legal

---

[2] Such as that suffered by Rebecca Schaeffer, who was murdered prior to the passage of the Act by a man who had obtained her home address from the California DMV. *See* 139 Cong. Rec. S15,761 (daily ed. Nov. 16, 1993) (statement of Sen. Barbara Boxer, a sponsor of the Act).

[3]Such as that suffered by individuals in Oregon recently victimized by a criminal who obtained a portion of the DMV database. *See* Natalie Brand, *Police Say Convicted Felon Charged with 50 Counts of ID Theft*, Fox Oregon (Mar. 24, 2012).

[4] The full text of that provision states:

> (4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of

scholars urge the Court to narrowly construe this exception and other such exceptions in federal privacy statutes. The records protected by the DPPA include the personal information used to authenticate identity as well as copies of the identifying documents themselves. *See infra* Part I. Identity thieves target this information maintained by the state agencies. *See infra* Part II.A. Data brokers use the data that individuals are required to provide to the state to create secret profiles. *See infra* Part II.B.

In order to safeguard the privacy of Americans, the Act's statutory exceptions should be interpreted narrowly and the definition of "personal information" should be interpreted broadly. *See infra* Part III.

I. State DMVs Collect Detailed, Sensitive Personal Information

State departments of motor vehicles ("DMVs") collect personal information from millions of Americans. At the time the DPPA was enacted, the DMV's collected names, addresses, and other identifying information. Following the enactment of the REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (2005), states collected even more information, including Social Security numbers ("SSNs") and biometric data.

---

litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

A. When the DPPA Was Enacted, Motor Vehicle Records Contained a Wide Range of Personal Information

When Congress passed the DPPA in 1994, state DMVs already collected a significant amount of personal information. As the Court noted in *Reno v. Condon*, 528 U.S. 141 (2000):

> State DMVs require drivers and automobile owners to provide personal information, which may include a person's name, address, telephone number, vehicle description, Social Security number, medical information, and photograph, as a condition of obtaining a driver's license or registering an automobile.

Id. at 143. Congress was understandably concerned about unrestricted access to this detailed personal information.[5] As the Court further explained:

---

[5] "Random access to personal information contained in DMV files poses a threat to every licensed driver in the Nation. In my own State of Virginia, over 127,815 requests are made every year for personal information contained in motor vehicle files. In Virginia, like most other States, licensees are not notified that their personal information has been accessed." 139 Cong. Rec. E2747 (daily ed. Nov. 3, 1993) (statement of Rep. James Moran, a sponsor of the Act). "[The DPPA] applies to auto titles, to car registrations, to driver's licenses, auto tags -- all this is open. There is a war in this country to fight for privacy. People are now fighting, and this [Act] is coming to their assistance to provide the privacy, which I and many others thought existed." 139 Cong. Rec. S15,764 (daily ed. Nov. 16, 1993) (statement of Sen. John Warner, a sponsor of the Act).

> The DPPA establishes a regulatory scheme that restricts the States' ability to disclose a driver's personal information without the driver's consent. 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).

Id. at 143.

After initial passage, and aware of the growing concern about the sale of personal information by DMVs, Congress amended the Act to require express consent to solicitation. *See* Pub. L. No. 106-69, 113 Stat. 986, §§ 350(c), (d), and (e) (1999).[6] As the Court further explained in *Reno*, "Under the amended DPPA, States may not imply consent from a driver's failure to take advantage of a state-afforded opportunity to block disclosure, but must rather obtain a driver's affirmative consent to disclose the driver's personal information for use in surveys, marketing, solicitations, and other restricted purposes. *Reno,* 528 U.S. 144-45.

---

[6] The author of the amendment said that "there should be a presumption that personal information will be kept confidential, unless there is compelling state need to disclose that information." 145 Cong. Rec. 23,699 (Oct. 4, 1999) (statement of Sen. Richard Shelby).

But today the amount of personal information collected by the state agencies is simply staggering. According to Department of Homeland Security ("DHS") regulations, state departments of transportation, and the American Association of Motor Vehicle Administrators,[7] the information held by DMVs includes:

- full names,[8]
- dates of birth,[9]
- gender,[10]
- driver's license numbers,[11]
- digital photos (often used with facial recognition technology),[12]

---

[7] The American Association of Motor Vehicle Administrators ("AAMVA") is a nonprofit organization that works closely with state and federal agencies to develop programs and standards for motor vehicle administration. Agencies often adopt these programs and standards directly into their regulatory regimes.

[8] *See e.g.* REAL ID Driver's Licenses and Identification Cards, 6 C.F.R. § 37.17(a) (2008). In accordance with the REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (2005), DHS issued a final rulemaking setting national standards for driver's licenses and identification cards. DHS's REAL ID rules have been finalized, but full compliance is not required until Jan. 15, 2013. 6 C.F.R. § 37.51 (2011).

[9] 6 C.F.R. § 37.17(b) (2008); *id.* at § 37.11(d).

[10] *Id.* at § 37.17(c).

[11] *Id.* at § 37.17(d).

[12] *Id.* at § 37.17(e). Even if a DMV does not issue a license, the regulations require the state to keep the photo on file for at least five years. *Id.* at § 37.11(a)(1). Thirty-eight jurisdictions use facial recognition technology. Am. Assoc. of Motor Vehicle Admin., *Biometrics in AAMVA Community* (2012), *available at*

- iris data,[13]
- addresses,[14]
- signatures,[15]
- SSNs,[16]
- copies of passports,[17]
- copies of birth certificates,[18]
- citizenship status and immigration documentation,[19]
- W-2 and 1099 tax records,[20]
- height,[21]

---

http://www.aamva.org/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=2497&libID=2483.

[13] 6 C.F.R. § 37.17(e)(iii) (2008); *Id.* at § 37.17(e)(iv). Irises contain biometric data that can be used to identify an individual.

[14] *Id.* at § 37.17(f); *id.* at § 37.11(f).

[15] *Id.* at § 37.17(g). Signatures contain biometric data about an individual's handwriting.

[16] *Id.* at § 37.11(e). Under the REAL ID program, driver's license applicants must submit SSNs to verify their identity.

[17] *Id.* at § 37.11(c)(i). Passports are used for identity and citizenship verification.

[18] *Id.* at § 37.11(c)(ii). Birth certificates are used for identity and citizenship verification. *See also* Fl. Dep't of Highway Safety and Motor Vehicles, *If You Do Not Have a Social Security Number*, http://www.gathergoget.com/SSN.aspx (last accessed Nov. 12, 2012) [hereinafter Fl. DMV, *SSN Alternatives*].

[19] 6 C.F.R. § 37.11(c)(iii)-(viii) (2008); *id.* at § 37.11(g). The REAL ID program requires applicants to prove that they are in the U.S. legally in order to obtain a driver's license or identity card.

[20] *Id.* at § 37.11(e)(i)-(ii). In the absence of a Social Security card, these documents are used to prove identity.

- eyesight,[22]
- place of birth,[23]
- weight,[24]
- military status,[25]

---

[21] Am. Assoc. of Motor Vehicle Admin., *Personal Identification - AAMVA North American Standard - DL/ID Card Design* 10 (June 2012), *available at* http://www.granddriver.info/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=2458&libID=2444 [hereinafter *DL/ID Card Design 2012*].

[22] *Id.* at 10. Eyesight is typically measured to determine if a driver must be restricted to wearing corrective glasses or lenses while driving. Such restrictions are then noted on the license. *See, e.g.* Minn. Dep't of Pub. Safety, *Just the Facts: New to Minnesota* (Aug. 2012), *available at* https://dps.mn.gov/divisions/dvs/forms-documents/Documents/NewResident.pdf; N.Y. Dep't Motor Vehicles, *Original Driver License* (Apr. 2011), *available at* http://www.dmv.ny.gov/forms/ccrp1.pdf [hereinafter N.Y. DMV, *Original Driver License*] (describing eye test requirement); Fl. Dep't of Highway Safety and Motor Vehicles, *Report of Eye Exam* (June 2011), *available at* http://www.flhsmv.gov/hsmvdocs/vision.pdf.

[23] *DL/ID Card Design 2012*, *supra* note 21, at 11.

[24] *Id.* at 12.

[25] *Id.* at 14. Some jurisdictions may list veteran status on a driver's license or give special registrations to active duty service members. Military orders or documentation are also used for identity and residency verification. *See, e.g.* Ala. Dep't of Pub. Safety, *Document Requirements And Fees* (2012), http://dps.alabama.gov/Home/wfContent.aspx?ID=30&PLH1=plhDriverLicense-DocumentRequirementsAndFees#ID; Colo. Dep't of Revenue, *Identification Requirements* (Apr. 27, 2011), *available at* http://www.colorado.gov/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobkey=id&blobtable=MungoBlobs&blobwhere=1251714422992&ssbinary=true; Minn. Dep't of Pub.

- radio frequency identification device ("RFID") data from enhanced driver's licenses,[26]
- fingerprints,[27]
- driver accident records,[28]
- traffic violations,[29]
- DUI convictions,[30]
- child support violations,[31]

Safety, *Identification Requirements* (Aug. 2012), *available at* https://dps.mn.gov/divisions/dvs/forms-documents/Documents/IdentificationRequirements_English.pdf; S.C. Dep't of Motor Vehicles, *United States Citizens Checklist for First Time Issuance of Driver's License, Beginner's Permit, and Identification Cards* (Mar. 2012), *available at* http://www.scdmvonline.com/DMVNew/forms/MV-93.doc [hereinafter S.C. DMV, *Checklist*]; N.Y. Dep't. of Motor Vehicles, *Proofs of Identity* (Oct. 2011), *available at* http://www.dmv.ny.gov/forms/id44.pdf [hereinafter N.Y. DMV, *Proofs of Identity*] (listing types of documents acceptable to prove identity); Fl. Dep't of Highway Safety and Motor Vehicles, *Titles & Registrations for Military Members* (2008), http://www.flhsmv.gov/dmv/forms/miltitle.html [hereinafter Fl. DMV, *Military Registrations*].

[26] *DL/ID Card Design 2012*, *supra* note 21, at 93-97. Four jurisdictions use RFID: Michigan, New York, Vermont, and Washington. Am. Assoc. of Motor Vehicle Admin., *US License Technology* (June 2011), *available at* http://www.aamva.org/ID-Security-Technologies/.

[27] Nine jurisdictions currently collect fingerprints. *Biometrics in AAMVA Community*, *supra* note 12.

[28] REAL ID Driver's Licenses and Identification Cards, 6 C.F.R. § 37.33(a)(4) (2008). *See also, e.g.* N.Y. Dep't. of Motor Vehicles, *Abstract of Driving Record* (Feb. 2012), *available at* http://www.dmv.ny.gov/forms/ds2421.pdf.

[29] *Id*.

[30] *Id*.

- court documents and pending prosecutions,[32]
- medical and mental health records,[33]
- vehicle title information and vehicle identification number ("VIN"),[34]

---

[31] *See*, *e.g.*, N.Y. Dep't. of Motor Vehicles, *Abstract of Driving Record*, *supra* note 28.

[32] *See*, *e.g.,* Ala. Dep't of Pub. Safety, *Star ID: Document List* (2012), http://dps.alabama.gov/Home/wfContent.aspx?ID=80&PLH1=plhDriverLicense-StarIDDocumentList; Colo. Dep't of Revenue, *Exception Processing* (2012), http://www.colorado.gov/cs/Satellite?c=Page&cid=1206604921186&pagename=Revenue-MV%2FRMVLayout; N.Y. Dep't. of Motor Vehicles, *Abstract of Driving Record*, *supra* note 28

[33] Medical and mental health evaluations that pertain to a driver's ability to operate a motor vehicle can form part of a person's motor vehicle record. *See, e.g.* Colo. Dep't of Revenue, *Exception Processing*, *supra* note 32; Minn. Dep't of Pub. Safety, *Just the Facts: Medical Conditions & Your Driver's License* (May 2011), *available at* https://dps.mn.gov/divisions/dvs/forms-documents/Documents/MedicalConditions_and_YourLicense.pdf ; N.Y. Dep't. of Motor Vehicles, *Physician's Reporting Form* (Dec. 2010), *available at* http://www.dmv.ny.gov/forms/ds6.pdf; Fl. Dep't of Highway Safety and Motor Vehicles, *Medical Reporting Form* (May 2012), *available at* http://www.flhsmv.gov/forms/72190.pdf.

[34] *See, e.g.* Minn. Dep't of Pub. Safety, *Just the Facts: New to Minnesota*, *supra* at note 22; Nat'l Motor Vehicle Title Info. Sys., *Consumer Access Product Disclaimer* (June 21, 2012), *available at* http://www.vehiclehistory.gov/CAPDisclaimer062112.pdf [hereinafter NMVTIS, *Consumer Access Product Disclaimer*]. The National Motor Vehicle Title Information System ("NMVTIS") serves as a nationwide electronic database of vehicle information, linking together state DMVs. *See also* Am. Assoc. of Motor Vehicle Admin., *State Vehicle Record Requests* (July 31, 2012) *available at* http://www.aamva.org/workarea/downloadasset.aspx?id=2701.

- vehicle history (including prior owners' personal information),[35]
- liens on car titles,[36]
- location data from vehicle smart cards,[37]
- license plate numbers,[38]
- vehicle and homeowner insurance information,[39]
- utility bills,[40]

---

[35] *See*, *e.g.*, NMVTIS, *Consumer Access Product Disclaimer*, *supra* note 34.

[36] *See*, *e.g.*, Minn. Dep't of Pub. Safety, *Just the Facts: New to Minnesota*, *supra* at note 22; NMVTIS, *Consumer Access Product Disclaimer*, *supra* note 34.

[37] *See, e.g.* Am. Assoc. of Motor Vehicle Admin., *ID Security Technologies: Smart Cards, available* at http://www.aamva.org/ID-Security-Technologies/ (last accessed Nov. 9, 2012). Smart cards used for tollbooth fee collection, such as the E-Z Pass used in the northeastern United States, use RFID transmitters with unique identifiers to record every time a specific vehicle passes through a tollbooth. Such records include both the time and location of each fee collected. In 2011, E-Z Pass transponders were used in 2.4 billion tollbooth transactions. E-Z Pass Group, *E-Z Pass Data 2005-2011* (2011), *available at* http://www.e-zpassiag.com/about-us/statistics.

[38] *See, e.g. State Vehicle Record Requests*, *supra* note 34.

[39] See, e.g. Ala. Dep't of Pub. Safety, *Star ID: Document List* , *supra* note 33; Colo. Dep't of Revenue, *Identification Requirements*, *supra* note 26; NMVTIS, *Consumer Access Product Disclaimer*, *supra* note 34; N.Y. Dep't Motor Vehicles, *Request for Insurance Information for NY Registrants Involved in An Accident* (Mar. 2011), available at http://www.dmv.ny.gov/forms/fs25.pdf.; N.Y. Dep't Motor Vehicles, *Proofs of Identity, U.S. Citizenship and NYS Residence* (Apr. 2011), available at http://www.dmv.ny.gov/forms/id44edl.pdf [hereinafter N.Y. DMV, *Proofs of ID - EDL*] (homeowner's/renter's insurance used to establish residency); S.C. DMV, *Checklist*, *supra* note 26.

- welfare, Medicaid, and food stamp records,[41]
- firearms permits,[42]
- professional licenses,[43]
- Native American tribal affiliations,[44]
- college and high school records,[45]
- union affiliation,[46]

---

[40] Utility bills are often used to establish identity and residency. *See, e.g.* Ala. Dep't of Pub. Safety, *Star ID: Document List* , *supra* note 32; Colo. Dep't of Revenue, *Identification Requirements*, *supra* note 25; N.Y. DMV, *Proofs of Identity*, *supra* note 25. REAL ID requires states to keep copies of documents used in driver's license or identity card applications for seven to ten years, depending on format. REAL ID Driver's Licenses and Identification Cards, 6 C.F.R. § 37.31(a) (2008) (describing source document retention).

[41] *See, e.g.* N.Y. DMV, *Proofs of Identity*, *supra* note 25; S.C. DMV, *Checklist*, *supra* note 26. Welfare, Medicaid, and food stamp documentation can be used to establish identity.

[42] Firearms permits, because they are issued by the state, are useful for establishing identity. Fl. DMV, *SSN Alternatives*, *supra* note 18; Minn. Dep't of Pub. Safety, *Identification Requirements* (Aug. 2012), *supra* note 25; N.Y. DMV, *Proofs of Identity*, *supra* note 25; S.C. DMV, *Checklist*, *supra* note 25.

[43] *See, e.g.* N.Y. DMV, *Proofs of Identity*, *supra* note 25; S.C. DMV, *Checklist*, *supra* note 25. Other types of state-issued licenses are useful for establishing identity.

[44] Tribal ID cards are used to prove identity. *See*, *e.g.*, Minn. Dep't of Pub. Safety, *Identification Requirements* (Aug. 2012), *supra* note 25; N.Y. DMV, *Proofs of Identity*, *supra* note 25.

[45] New York requires college and high school students to submit transcripts or report cards in addition to school ID cards. *Id. See also* Ala. Dep't of Pub. Safety, *Document Requirements And Fees*, *supra* note 25; Colo. Dep't of Revenue, *Identification Requirements*, *supra* note 26; Fl. DMV, *SSN Alternatives*, *supra* note 18; Minn. Dep't of Pub. Safety, *Identification Requirements* (Aug. 2012), *supra* note 25; S.C. DMV, *Checklist*, *supra* note 25.

- health insurance documentation,[47]
- life insurance documentation,[48]
- banking and credit card records,[49]
- marriage licenses and divorce records,[50]
- deeds, mortgages, and rental leases,[51]
- nursing home documentation,[52]

---

[46] *See, e.g.* N.Y. DMV, *Proofs of Identity*, *supra* note 25. Union cards are used to prove identity

[47] Health insurance cards are used to prove identity. *See, e.g.,* Ala. Dep't of Pub. Safety, *Document Requirements And Fees*, *supra* note 25; Colo. Dep't of Revenue, *Exception Processing*, *supra* note 32; N.Y. DMV, *Proofs of Identity*, *supra* note 25; S.C. DMV, *Checklist*, *supra* note 25.

[48] Life insurance policies are used to prove identity. *See*, *e.g.*, N.Y. DMV, *Proofs of Identity*, *supra* note 25. *See also* Fl. DMV, *SSN Alternatives, supra* note 18.

[49] Bank statements, cancelled checks, ATM cards, and credit cards can be used to establish identity. *See*, *e.g.*, Colo. Dep't of Revenue, *Identification Requirements*, *supra* note 26; N.Y. DMV, *Proofs of Identity*, *supra* note 25; S.C. DMV, *Checklist*, *supra* note 25.

[50] Marriage and divorce records are used to establish identity and to change one's surname on an existing license. *See*, *e.g.*, Ala. Dep't of Pub. Safety, *Document Requirements And Fees*, *supra* note 25; Colo. Dep't of Revenue, *Exception Processing*, *supra* note 32; Minn. Dep't of Pub. Safety, *Identification Requirements* (Aug. 2012), *supra* note 25; N.Y. DMV, *Proofs of Identity*, *supra* note 25.

[51] Property records are used to establish residency. *See, e.g.* Ala. Dep't of Pub. Safety, *Star ID: Document List* , *supra* note 33; Colo. Dep't of Revenue, *Identification Requirements*, *supra* note 26; N.Y. DMV, *Proofs of Identity – EDL*, *supra* note 18; S.C. DMV, *Checklist*, *supra* note 25.

[52] A nursing home or assisted living statement can be used to establish residency. *See*, *e.g.*, N.Y. DMV, *Proofs of Identity – EDL*, *supra* note 18.

- jury duty records,[53]
- property tax receipts,[54]
- voter registration documentation,[55]
- Selective Service records,[56]
- religious affiliation records,[57]
- internet protocol (IP) addresses used to log on to DMV websites,[58]

---

[53] Jury duty summons can be used to establish residency. *Id.*

[54] Property tax receipts can be used to establish residency. *Id.*

[55] Voter registration cards can be used to establish residency or identity. *See*, *e.g.*, Ala. Dep't of Pub. Safety, *Star ID: Document List* , *supra* note 33; Colo. Dep't of Revenue, *Voter Registration* (2012), http://www.colorado.gov/cs/Satellite/Revenue-MV/RMV/1211361061109; Fl. DMV, *SSN Alternatives*, *supra* note 18; N.Y. DMV, *Proofs of Identity – EDL*, *supra* note 18. Forty-four jurisdictions participate in the Help America Vote Verification ("HAVV") program, which uses motor vehicle records to verify voter registration information. Am. Assoc. of Motor Vehicle Admin., *Help America Vote Verification (HAVV) - Participants*, http://www.aamva.org/HAVV/ (last accessed Nov. 12, 2012).

[56] Selective Service draft cards can be used to establish residency or identity. *See, e.g.* Ala. Dep't of Pub. Safety, *Document Requirements And Fees*, *supra* note 25; Fl. DMV, *SSN Alternatives, supra* note 18; N.Y. DMV, *Proofs of Identity – EDL*, *supra* note 18.

[57] Baptism certificates and family bible records can be used to verify identity. See, e.g. Colo. Dep't of Revenue, *Exception Processing*, *supra* note 32; Fl. DMV, SSN Alternatives, supra note 18.

[58] *See, e.g.* Mass. Dep't. of Trans. Registry of Motor Vehicles, *Driving Record : User Agreement* (2012), https://secure.rmv.state.ma.us/DrvRecords/Intro.aspx (proceed to User Agreement via "Continue" button). The Massachusetts Registry of Motor Vehicles (RMV) collects the Internet Protocol ("IP") addresses of those who request their driving record

- adoption records,[59]
- felon or parolee identification documents,[60]
- records of homelessness or domestic violence,[61]
- location data from red light cameras,[62] and
- location data from license plate readers.[63]

---

through the RMV's website. The RMV matches the IP addresses with personally identifiable information when reasonable for a criminal investigation or public safety. *See also* Cal. Dep't of Motor Vehicles, *Conditions* (2011), http://www.dmv.ca.gov/portal/portal/conditions.htm (outlining conditions of using the CA DMV website, including collection of IP addresses).

[59] *See*, *e.g.*, Ala. Dep't of Pub. Safety, *Document Requirements And Fees*, *supra* note 25; Minn. Dep't of Pub. Safety, *Identification Requirements* (Aug. 2012), *supra* note 25.

[60] *See*, *e.g.*, Ala. Dep't of Pub. Safety, *Document Requirements And Fees*, *supra* note 25; Colo. Dep't of Revenue, *Identification Requirements*, *supra* note 26; S.C. DMV, *Checklist*, *supra* note 25.

[61] *See*, *e.g.*, S.C. DMV, *Checklist*, *supra* note 25.

[62] Red light camera pictures reveal the specific time, date, and location of an individual. *See*, *e.g.*, *Wemhoff v. D.C.*, 887 A.2d 1004 (D.C. Ct. App. 2005).

[63] License plate readers record time, date, and location when they scan an individual's plate. *See*, *e.g.*, City of Beverly Hills, *ALPR Mobile Camera Systems/Multiple System Option: Legal Notice - Bids Wanted*, at 11 (Oct. 22, 2012), *available at* http://www.beverlyhills.org/cbhfiles/storage/files/1348456519262014121/ALPRFixedSiteBid2-1MulticameraSystemPDFcopy.pdf (requesting bids for a mobile camera system that can "cross-link license plate data from external systems, such as DMV records"); Press Release, Va. Dep't of Motor Vehicles, Plate Readers Offer Advanced Inspection System for Trucks (Feb. 22, 2012), *available at*

After collecting personal information through DMVs, state and federal agencies pool motor vehicle records for inter-jurisdictional use. Some programs create national databases of motor vehicle records, while others use motor vehicle records to authenticate identities. The Commercial Driver's License Information System allows all DMVs nationwide to share motor vehicle records and maintain one complete driving record for an individual. Am. Assoc. of Motor Vehicle Admin., *Commercial Driver's License Information System (CDLIS)*.[64] The National Highway Traffic Safety Administration administers the National Driver Register, a nationwide database aggregating state DMV information about "problem drivers," in part to help employers make hiring decisions. Nat'l Highway Traffic Safety Admin., *National Driver Register (NDR)*.[65] Twenty-three jurisdictions connect motor vehicle records through the Digital Image Access and Exchange program. Am. Assoc. of Motor Vehicle Admin., *Digital Image Access and Exchange (DIA)*.[66]

---

http://www.dmv.state.va.us/webdoc/general/news/news.asp?id=6614.

[64] http://www.aamva.org/CDLIS/ (last accessed on Nov. 13, 2012).

[65] http://www.nhtsa.gov/Data/National+Driver+Register (last accessed on Nov. 13, 2012). The NDR contains information on license suspensions and revocations, DUI violations, and other serious traffic violations.

[66] http://www.aamva.org/Digital-Image-Access-and-Exchange/ (last accessed Nov. 13, 2012). Participants include: Alaska, Arizona, the District of Columbia, Hawaii, Idaho, Illinois, Kansas, Kentucky, Maryland, Massachusetts, Missouri, Nebraska, Nevada, New Mexico, North Dakota, Ohio,

Through the Help America Vote Verification (HAVV) program, forty-four jurisdictions verify voter registration information using motor vehicle records. Am. Assoc. of Motor Vehicle Admin., *Help America Vote Verification (HAVV)*.[67] The National Motor Vehicle Title Information System links together DMV motor vehicle records through a nationwide electronic database of vehicle information. See Nat'l Motor Vehicle Title Info. Sys., www.vehiclehistory.gov (last visited Nov. 14, 2012).

B. DHS REAL ID Regulations Compel State DMVs to Collect Far More Personal Information Than Before

The REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (2005), significantly expanded the scope of information contained in motor vehicle records. DMVs now collect many of the types of information described above in order to comply with DHS REAL ID regulations.

REAL ID sets standards for state driver's licenses intended to be used for federal purposes, such as passing through airport security checkpoints. REAL ID Driver's Licenses and Identification Cards, 6 C.F.R. § 37.1 (2008). In order to ensure that only legal U.S. persons have access to driver's licenses and identification cards, the regulations require applicants produce various documents related to citizenship, identity, and residency. *Id.* at § 37.11. "A

Pennsylvania, South Dakota, Tennessee, Virginia, Washington, West Virginia, and Wyoming.

[67] http://www.aamva.org/HAVV/ (last accessed on Nov. 13, 2012).

DMV may issue a REAL ID driver's license or identification card only to a person who has presented satisfactory evidence of lawful status." *Id.* at § 37.11(g) (referring to lawful immigration status or U.S. citizenship). As a consequence, DMVs now collect critical documents that establish identity, including birth certificates, passports, permanent resident cards, and IRS tax filings. *See* 6 C.F.R. § 37.11 (2008). State DMVs must verify application materials through central databases, *id.* at § 37.13, and retain copies of application materials for at least seven to ten years. *Id.* at § 37.31. Even if no license is issued, a state must retain digital photos of applicants for a minimum of five years. *Id.* at § 37.11(a)(1). When the DMV does issue a driver's license compliant with REAL ID, the card must meet specific requirements for security, *id.* at § 37.15, and contain certain categories of information. *Id.* at § 37.17.

Congress enacted the DPPA prior to the enactment of REAL ID. Yet even before the REAL ID requirements existed,[68] motor vehicle records contained sensitive personal data. Once state DMVs become fully compliant with the REAL ID

---

[68] As EPIC previously discussed in its comprehensive REAL ID report, the requirements set by DHS insufficiently protect cardholder data. "[A]s part of the cost-saving effort, Homeland Security decided not to encrypt the data that will be stored on the card." EPIC, *REAL ID Implementation Review: Few Benefits, Staggering Costs* 3-4 (May 2008), available at https://epic.org/privacy/id_cards/epic_realid_0508.pdf.

requirements,[69] they will acquire, retain, and disclose an even broader spectrum of information.

C. Motor Vehicle Records Contain SSNs, Which Are Widely Used for Both Identification and Authentication

Private and public organizations frequently use SSNs to administer programs, verify eligibility for services, and conduct efficacy research. Cynthia M. Fagnoni, U.S. Gov't Accountability Office, GAO-06-586T, *Social Security Numbers: More Could Be Done to Protect SSN*s 1 (2006).[70] All state DMVs are required to collect SSNs under the REAL ID regulations. 6 C.F.R. § 37.11(e). These unique identifiers are also used by other state and local agencies, courts, healthcare organizations, credit rating agencies, banks, telecommunications companies, accountants, third-party contractors, and data brokers, among others. *Id.* at 4. The Government Accountability Office ("GAO") found that SSNs are "widely exposed to view in a variety of public records." *Id.* at 14. Because SSNs are used for many purposes, they are valuable to those who wish to acquire credit, commit crimes, or masquerade as another person.

What makes SSNs especially sensitive is that organizations use them as both an identifier and an authenticator. This means that in some contexts, the SSN will be used to verify identity (such as with

---

[69] REAL ID full compliance is not required until Jan. 15, 2013. 6 C.F.R. § 37.51 (2011).

[70] A*vailable at* http://www.gao.gov/new.items/d06586t.pdf.

driver's license applications), while in other contexts the SSN will be used as a password (as is often the case in the financial services sector).[71] This dual-use of SSNs creates insecurity, similar to a situation where an individual's username and password are identical. The GAO reported that "[g]iven the significance of the SSN in committing fraud or stealing a person's identity, it is imperative that steps be taken to protect it. Without proper safeguards in place, SSNs will remain vulnerable to misuse, thus adding to the growing number of identity theft victims." Fagnoni at 17.

D. Motor Vehicle Records Now Contain Biometric Data, Which Are Both Unique and Immutable

Motor vehicle records also contain a plethora of biometric data. Biometric data include immutable physical characteristics that can substantially or uniquely identify an individual. New techniques attempt to automate the process of identification by comparing certain human features with records stored in digital databases, such as state DMV records.[72] Facial recognition, for example, extracts a human face from a scene, measuring points on the face (such as the distance between the eyes, or the shape of cheekbones), and then comparing the

---

[71] *See generally*, EPIC, *Social Security Numbers*, *available at* https://epic.org/privacy/ssn/ (last accessed Nov. 9, 2012).

[72] *See generally*, EPIC, *Biometric Identifiers*, https://epic.org/privacy/biometrics/ (last accesed Nov. 9, 2012).

measurements to a database of digital pictures.[73] DMV driver's license photos often supply those databases. *See* Anil K. Jain and Brendan Klare, *Matching Forensic Sketches and Mug Shots to Apprehend Criminals*, 44 IEEE Computer, no. 5, May 2011, at 84-86.[74]

The types of biometric data held in motor vehicle records include fingerprints, facial photos, and iris data. Nine jurisdictions use fingerprints in their motor vehicle records, while thirty-eight jurisdictions use some form of facial recognition technology. Am. Assoc. of Motor Vehicle Admin., *Biometrics in AAMVA Community 2012*.[75] REAL ID mandates that irises (another unique identifier similar to fingerprints) be clearly visible in DMV digital photos. 6 C.F.R. § 37.17(e)(iii)-(iv) (2008).

Because biometric data are immutable characteristics, their use creates additional risks to personal privacy. The National Research Council reports, "[t]he key social issue surrounding biometrics is the seemingly irrevocable link between biometric traits and a persistent information record about a person. Unlike most other forms of recognition, biometric techniques are firmly tied to our physical bodies." Nat'l Research Council, *Biometric Recognition: Challenges and Opportunities*,

---

[73] *See generally* EPIC, *Face Recognition*, https://epic.org/privacy/facerecognition/.

[74] *Available at* http://www.cse.msu.edu/~klarebre/docs/IEEE_Comp_Sketch.pdf.

[75] *Available at* http://www.aamva.org/ID-Security-Technologies/.

85 (Joseph N. Pato and Lynette I. Millett eds., The National Academies Press 2010).

The biometric records held by state DMVs create a bridge between one's publicly available biometric data and non-publicly available personal information.[76] Individuals typically cannot control the release of their biometric information. Biometrics can be collected without a person's consent, or even knowledge. One's picture can be taken on any public street. One's fingerprint can be lifted from any commonplace surface. With commercially available high-resolution cameras, even the details of one's irises can be easily photographed.[77] Given the increased risks to privacy of public disclosure of immutable physical characteristics maintained by state agencies, the Court should consider carefully the consequences of broadly interpreting an exception in a privacy statute that would otherwise safeguard this information.

---

[76] For example, in California, fingerprints are protected "personal information," yet fingerprinting is not a per se infringement of one's right to privacy. *See Perkey v. Dep't of Motor Vehicles*, 42 Cal.3d 185 (Cal. 1986).

[77] For a discussion of the cultural, social, and legal risks associated with biometric data, s*ee generally* Nat'l Research Council, *Biometric Recognition: Challenges and Opportunities*, 85-115 (Joseph N. Pato and Lynette I. Millett eds., The National Academies Press 2010).

II. Identity Theft and Security Breaches Threaten the Privacy of Motor Vehicle Records

According to the Federal Trade Commission, identity theft is the number one concern of American consumers. Press Release, Fed. Trade Comm'n, *FTC Releases Top Complaint Categories for 2011: Identity Theft Once Again Tops the List* (Feb. 28, 2012).[78] Identity thieves cause substantial financial injury to Americans by exploiting motor vehicle records. An important first step in preventing identity theft is securing the enrollment documents, such as records of birth, that provide the basis for authentication. The DPPA is the primary legal mechanism that protects these records.

Motor vehicle records are also at risk when they are transferred from DMVs to third party databases, such as those maintained by major data brokers. The Congressional Bipartisan Privacy Caucus recently opened an investigation into data broker industry practices in an attempt to increase transparency and protect personal information. *See* Natasha Singer, *Congress to Examine Data Sellers*, N.Y. Times, Jul. 24, 2012, at B1. The disclosure of motor vehicle records to data brokers has resulted in identity thieves accessing "personal information from more than 145,000 consumers" in 2005. *See ChoicePoint Settles Data Security Case*, Reuters, June 1, 2007.

---

[78] http://ftc.gov/opa/2012/02/2011complaints.shtm.

A. Identity Thieves Target Motor Vehicle Records to Obtain Personal Information

State DMVs recognize that identity theft is a significant problem. The California Department of Motor Vehicles notes that "[i]dentity theft and identity fraud are two of the fastest growing crimes in the United States." Cal. Dep't of Motor Vehicles, *Identity Fraud* (Apr. 2010).[79] As a result, state DMVs recognize that access to "confidential information such as your Social Security number" must be "highly restricted." Or. Dep't of Transp., *Identity Theft*.[80] Some state DMVs have even added specific provisions to protect SSNs. *See*, *e.g.*, Pa. Dep't of Transp., *Social Security Number Fact Sheet* (Oct. 2008);[81] N.Y. Dep't of Motor Vehicles, *Driver's Privacy Protection Act Frequently Asked Questions*.[82] States recognize that a "strong collaborative effort" is necessary to mitigate "the risk for fraud and identity theft." Pa. Dep't of Transp., *Reporting Fraud*.[83]

States stress the importance of the security of driver records. California has implemented advanced security measures to protect personal information. *See* Cal. Dep't of Motor Vehicles, *DMV and Your*

---

[79] http://www.dmv.ca.gov/pubs/brochures/fast_facts/ffdl25.htm (last accessed Nov. 13, 2012).

[80] http://www.oregon.gov/odot/dmv/pages/driverid/idtheft.aspx (last accessed Nov. 13, 2012).

[81] *Available at* .http://www.dmv.state.pa.us/pdotforms/misc/ssfs.pdf.

[82] http://www.dmv.ny.gov/qaprive.htm (last accessed Nov. 13, 2012).

[83] http://www.dmv.state.pa.us/identity_theft/reporting/fraud.shtml (last accessed Nov. 13, 2012).

Information (2011).[84] This includes explicit limitations on employee access, disclosure, and alteration of personal information, as well as requiring that employees take "reasonable precautions" to prevent unauthorized use. *Id*. Wisconsin requires all employees to sign a contract promising to protect the privacy of the personal information contained in DMV records. *See* Wis. Dep't of Transp., *Recipient Employee Memorandum of Understanding Data Access to WisDot DMV Records* (Oct. 2009).[85]

The personal information of consumers is "the currency of identity theft." President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* 13 (Apr. 2007). State DMVs and third parties who obtain driver information are at risk because they hold the keys to fraud and identity theft. "SSNs, along with names and birth certificates, are among the three personal identifiers most often sought by identity thieves." U.S. Gov't Accountability Office, GAO-09-759T, *Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain* 8 (2009).[86]

---

[84] http://www.dmv.ca.gov/dl/authority.htm (last accessed Nov. 13, 2012).

[85] http://www.dot.wisconsin.gov/drivers/forms/pars-mou.pdf (last accessed Nov. 13, 2012).

[86] *Available at* http://gao.gov/assets/130/122769.pdf. Social Security Numbers (SSNs), personal information, and credit card data are the "crown jewel[s] for a cyberattacker." Robbie Brown, *Hacking of Tax Records Has Put States on Guard*, N.Y. Times, Nov. 5, 2012, at A17.

State DMV records have been targeted numerous times over the past decade, which has increased the risk of driver identity theft. In one case, a criminal in Oregon obtained possession of a significant portion of the DMV database and used the information to commit identity theft. Natalie Brand, *Police Say Convicted Felon Charged with 50 Counts of ID Theft*, Fox Oregon (Mar. 24, 2012). Recently in Massachusetts "[t]wo masked men stole several bags containing various records that included registration transactions, duplicate titles, crash reports, citation payments" and other state DMV records. Mark E. Vogler, *RMV Document Theft Prompts Identity Fraud Concerns*, Gloucester Times, Apr. 6, 2012. A similar theft of computers containing sensitive driver information occurred at a Connecticut DMV. Gregory B. Hladky, *3 Computers Stolen from DMV Held Personal Info*, New Haven Register, Dec. 21, 2007. The Colorado state DMV put more than three million drivers at risk by sending "large batches of personal information over the Internet without encryption" and failing to "properly limit access to its database." Jessica Fender, *DMV Puts Coloradans at Risk of ID Theft*, Denver Post, Jul. 9, 2008.[87] Even these unintentional acts can put personal information at risk.

States are pushing back against DHS REAL ID regulations in part out of concern that new linked databases "of all licensing information" will create a clear "target of identity theft." Eric Lipton, *Rebellion Growing as States Challenge a Federal Law to Standardize Driver's Licenses*, N.Y. Times, Feb. 5,

---

[87] *Available at* http://www.denverpost.com/news/ci_9822063.

2007.[88] This concern has proved valid, as cyber-attacks have recently targeted major centralized databases of personal information. Hackers recently attacked a South Carolina tax information system and stole 3.6 million SSNs and 387,000 credit and debit card numbers. Robbie Brown, *Hacking of Tax Records Has Put States on Guard*, N.Y. Times, Nov. 5, 2012, at A17. This attack and others highlight the risks state, federal, and private record systems that contain SSNs and other identifying data. These attacks also underscore the importance of federal privacy laws that seek to protect this information.

B. Data Brokers Put Motor Vehicle Records at Risk by Combining Them with Consumer Profiles

The personal information contained in motor vehicle records, which state law requires consumers to provide, is increasingly at risk not only in DMV databases but also in the systems of large data brokers. Data brokers are modern "data refineries" that collect and mine personal information stored in government and private sector records. *See* Natasha Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times, June 16, 2012, at B1. These data brokers rely on state DMV and other government records to build comprehensive consumer

---

[88] *Available at* http://www.nytimes.com/2007/02/05/washington/05real.html. As a comprehensive law enforcement report recently noted, "[a]ll identity-related crime must begin, at some time, with the acquisition of valuable personal information by criminals." Dep't of Justice, *Identity-Related Crime: A Threat Assessment* 10 (November 2010).

profiles. *See*, *e.g.*, Letter from Axicom to Rep. Ed Markey, U.S. House of Representatives (Aug. 15, 2012);[89] Letter from Intelius to Reps. Edward J. Markey, Joe Barton, et al., U.S. House of Representatives (Aug. 22, 2012);[90] Michael Hiltzik, *Big Data Broker Eyes DMV Records*, L.A. Times, Dec. 1, 2005.

Identity thieves are eager to access the driver records contained in data broker systems, and they have succeeded in the past. In 2005, ChoicePoint "divulged the personal records of at least 162,000 individuals to a gang of Los Angeles identity thieves." Michael Hiltzik, *Big Data Broker Eyes DMV Records*, L.A. Times, Dec. 1, 2005. ChoicePoint eventually paid $500,000 to settle the claims of forty-four state attorneys general as a result of its failure to protect the sensitive consumer data. *ChoicePoint Settles Data Security Case*, Reuters, June 1, 2007. After the 2005 incident, ChoicePoint sought to obtain thirty

---

[89] *Available at* http://markey.house.gov/sites/markey.house.gov/files/documents/Acxiom.pdf. As Axicom states in its letter:

> [S]tate and federal government records such as real property and assessor records, *motor vehicle records*, *driver's license records*, professional licenses, other government issued licenses such as hunting and fishing licenses, voter records, and court records, including bankruptcies, liens, judgments, and criminal conviction records.

Id. at 10 (emphasis added).

[90] *Available at* http://markey.house.gov/sites/markey.house.gov/files/documents/Intelius.pdf.

million additional motor vehicle records from the California DMV. Michael Hiltzik, *Big Data Broker Eyes DMV Records*, L.A. Times, Dec. 1, 2005.

Recently the Congressional Bipartisan Privacy Caucus opened an investigation into data broker industry practices. Natasha Singer, *Congress to Examine Data Sellers*, N.Y. Times, July 24, 2012, at B1. This investigation is the result of a rising concern that "an unprecedented amount of personal, medical and financial information about people" is collected and used "to the potential detriment of consumers." Natasha Singer, *Senator Opens Investigation of Data Brokers*, N.Y. Times, Oct. 10, 2012, at B3. Yet the data brokers' responses to the investigation "offer only a glimpse of the practices an industry that has operated in the shadows for years." Press Release, Congressional Bi-Partisan Privacy Caucus, *Nine Major Data Brokers Provide Lawmakers with Only a Partial Glimpse of Industry Controlling Information on Hundreds of Millions of Americans* (Nov. 8, 2012).[91]

This lack of transparency by an industry that compiles and uses records obtained from state DMVs highlights the need for strong legal protections to limit misuse of driver information. Absent such protections, drivers currently have no way to limit the disclosure of records they are required by law to provide, which can lead to identity theft and abuse of their personal information.

---

[91] *Available at* http://markey.house.gov/press-release/lawmakers-release-information-about-how-data-brokers-handle-consumers'-personal.

III. In Order to Satisfy Congressional Intent and Safeguard Privacy, "Personal Information" Should Be Interpreted Broadly and DPPA Statutory Exceptions Should Be Interpreted Narrowly

This Court has recognized that large databases of personal information, maintained by state agencies, pose a significant threat to personal privacy. *See Whalen v. Roe*, 429 U.S. 589, 605-06 (1977) (noting "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files"). *See also*, *NASA v. Nelson*, 131 S. Ct. 746, 751 (2011) ("[w]e assume, without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen* and *Nixon*."). At the time Congress enacted the DPPA, the Act gave "people more control over the disclosure of their personal information." 139 Cong. Rec. S15,763 (daily ed. Nov. 15, 1993) (statement of Sen. Barbara Boxer, a sponsor of the Act). The DPPA directly incorporated "both the intent of the 1974 Privacy Act" as well as "the recommendations of the landmark 1977 Privacy Protection Study Commission report." 139 Cong. Rec. S15,764 (daily ed. Nov. 16, 1993) (statement of Sen. John Warner, a sponsor of the Act).

A. Based on the Text and Congressional Intent, The Definition of "Personal Information" Is Broad and Encompassing.

The DPPA defines "personal information" to. mean "information that identifies an individual,

including" numerous enumerated examples. 18 U.S.C. §2725(3).[92] This language implies that other, non-enumerated categories of information, such as biometric data or unique IP addresses, also fall within the definition if they could identify an individual. *See Fed. Land Bank of St. Paul v. Bismarck Lumber Co.,* 314 U.S. 95, 100 (1941) ("the term 'including' is not one of all-embracing definition, but connotes simply an illustrative application of the general principle").[93]

The statute's closed list definition of "highly restricted personal information" further illustrates the scope of the "personal information" definition. 18 U.S.C. § 2725(4).[94] "A provision that may seem ambiguous in isolation is often clarified by the remainder of the statutory scheme." *United Sav. Ass'n of Tex. v. Timbers of Inwood Forest Assoc.*, 484

---

[92] The full text of the definition states:

> "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.

[93] "[T]he word *include* does not ordinarily introduce an exhaustive list." Antonin Scalia and Bryan A. Garner, Reading Law: The Interpretation of Legal Texts 132 (2012) (emphasis in original).

[94] The full text of the definition states: "highly restricted personal information' means an individual's photograph or image, social security number, [and] medical or disability information."

U.S. 365, 371 (1988). Contrasting the "highly restricted personal information" closed list definition with the open list definition of "personal information" shows that the latter is more encompassing than merely its enumerated examples.

The expansive scope of "personal information" aligns with Congress' intent to safeguard driver's control over their own information. *See Reno v. Condon*, 528 U.S. 141, 143 (2000) (stating that Congress passed the DPPA after finding that many States sell individuals' personal information).

> Easy access to personal information makes every driver in this Nation vulnerable and infringes on their right to privacy. Government's duty is to keep citizens safe and it should not, therefore, be contributing to insecurity.

139 Cong. Rec. S15,765 (daily ed. Nov. 16, 1993) (statement of Sen. Charles Robb).[95] Almost twenty years after the enactment of the DPPA, the information DMVs possess has grown increasingly more sensitive. In order for Americans to maintain privacy and control over their own information, the definition of "personal information" must include new types of data that can identify an individual.

---

[95] "There is a war in this country to fight for privacy. People are now fighting, and this [Act] is coming to their assistance to provide the privacy, which I and many others thought existed." 139 Cong. Rec. S15,764 (daily ed. Nov. 16, 1993) (statement of Sen. John Warner, a sponsor of the bill).

B. The Scope of the Litigation Exception is Narrow and Does Not Permit Solicitation.

Limiting access to the sensitive information contained in motor vehicle records is the purpose of the DPPA. The D.C. Court of Appeals properly interpreted the (b)(4) litigation exception narrowly and protected the privacy of personal information in *Wemhoff v. D.C.,* 887 A.2d 1004 (D.C. Ct. App. 2005).[96] In that case, the court held that "acquiring personal information from the motor vehicle records for the purpose of finding and soliciting clients for a lawsuit is not a 'permissible use' within the meaning of § 2721(b)." *Id*. at 1012. That reading follows this Court's previous interpretation of the DPPA that States must "obtain a driver's affirmative consent to disclose the driver's personal information for use in surveys, marketing, solicitations, and other restricted purposes." *Reno v. Condon*, 528 U.S. 141, 145 (2000).

---

[96] *See* 18 U.S.C. § 2721(b)(4). The full text of that provision states:

> For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court.

CONCLUSION

For the foregoing reasons, *amici* respectfully ask this Court to reverse the decision of the Court of Appeals for the Fourth Circuit below.

Respectfully submitted,

MARC ROTENBERG
ALAN BUTLER
ELECTRONIC PRIVACY
INFORMATION
CENTER (EPIC)
1718 Connecticut Ave. NW
Suite 200
Washington, DC 20009
(202) 483-1140
rotenberg@epic.org

November 16, 2012