EPIC - Electronic Privacy Information Center

Focusing public attention on emerging privacy and civil liberties issues

The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record

- Introduction |
- DPPA's Provisions |
- News |
- Cases |
- Resources |
- Previous Top News

Top News

- **EPIC, Coalition Seek Privacy Safeguards for Car Data:** EPIC, joined by a coalition of privacy, consumer rights, and civil rights organizations, and members of the public, urged the National Highway Traffic Safety Administration to protect driver privacy and establish privacy safeguards for "event data recorders." The agency has proposed mandatory installation of "black boxes" in all cars and small trucks by 2014. Thirteen states have passed laws that limit the use of EDRs. EPIC recommended that the agency: (1) restrict the amount of data that EDRs collect; (2) conduct a comprehensive privacy impact assessment; (3) uphold Privacy Act protections; (4) require security standards for EDR data; and (5) establish best practices to fully protect the privacy rights of vehicle owners and operators. EPIC argued that it is contrary to reasoned decisionmaking for the agency to mandate massive data collection and not fully amend its current regulations to protect individual privacy. For more information, see EPIC: Event Data Recorders and Privacy and EPIC: The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record. (Feb. 12, 2013)
- **Supreme Court to Consider Law that Protects Privacy of Drivers' Records:** The Supreme Court is set to hear arguments in Maracich v. Spears, a case involving the Drivers' Privacy Protection Act. The Court agreed to hear the case after a lower could ruled that impermissible uses of personal data held by DMVs were "inextricably intertwined" with permissible uses. The Supreme Court previously said that the law "establishes a regulatory scheme that restricts the States' ability to disclose a driver's personal information without the driver's consent." EPIC filed an amicus curiae brief in support of the Petitioners, urging that the Court overturn the lower court's judgment. EPIC's brief details the staggering amount of personal information contained in driver records, particularly as a consequence of the REAL ID regulations. EPIC argues that "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." The EPIC amicus brief is joined by twenty-seven technical experts and legal scholars. For more information, see EPIC: Maracich v. Spears, EPIC: The Driver's Privacy Protection Act, and EPIC: National ID and REAL ID. (Jan. 8, 2013)

- **Federal Agency Proposes "Black Box" Mandate for Cars:** The National Highway Traffic Safety Administration has proposed that, beginning September 1, 2014, all new cars will be required to have Event Data Recorders. The devices record detailed information about drivers, which can be made available to insurance companies, the police, and others. Currently, there are minimal privacy protections in the draft regulation. The public will have until February 11, 2013 to provide comments to the agency. EPIC recommends that commentators urge the agency to "Strengthen privacy safeguards." For more information see EPIC - Event Data Recorders and Privacy and EPIC - Driver Privacy Protection Act. (Dec. 14, 2012)
- **EPIC Argues for Privacy of Driver's Records in Supreme Court Case:** In a "friend of the court" brief, EPIC has urged the U.S. Supreme Court to limit the disclosure of personal information covered by the Driver's Privacy Protection Act. At issue in Maracich v. Spears is a lower court's decision to allow disclosure of information stored in state departments of motor vehicles. EPIC's amicus brief details the staggering amount of personal information in driver's records, particularly as a consequence of the REAL ID regulations. In Reno v. Condon, the Supreme Court upheld the Constitutionality of the federal law. EPIC filed an amicus brief in that case and said "The 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." For more information, see EPIC: Maracich v. Spears and EPIC: The Driver's Privacy Protection Act. (Nov. 16, 2012)
- **Supreme Court to Hear Drivers' Records Privacy Case:** The US Supreme Court has decided to review Marachich v. Spears, a case concerning the Drivers' Privacy Protection Act. The federal privacy law prohibits the disclosure of personal information in state motor vehicle records, except under certain narrow circumstances. In 2000, several states challenged the law. EPIC argued in an amicus brief that "the 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 Supreme Court upheld the law. More recently, EPIC has argued that resellers of driver records should be strictly liable for violations of the law. At issue in the Marachich case is whether records can be disclosed to facilitate attorney solicitations. The Court of Appeals for the Fourth Circuit ruled that the law permits solicitations under the "litigation" exception. For more information, see EPIC: The Drivers' Privacy Protection Act and EPIC: Gordon v. Softech. (Sep. 25, 2012)
- **Government Standard for Vehicle "Event Data Recorders" Will Go Forward:** The National Highway Traffic Safety Administration has denied a petition for rulemaking that would delay the effective date of national requirements for event data recorders. The government requirements for the devices that are installed in vehicles will be effective on September 1, 2012. Commonly referred to as "black boxes," event data recorders collect and store vehicle operation information before, during, and after a vehicle crash, including vehicle location, driver speed, seat belt use, and number of vehicle occupants. In 2003 and 2004, EPIC urged the agency and the automotive industry to protect privacy interests when deploying event data recorders. For more information on driver privacy, see EPIC: The Drivers Privacy Protection Act. (Aug. 17, 2012)
- **Federal Appeals Court Holds that Driver's Privacy Law Applies to Parking Tickets:** The Seventh Circuit Court of Appeals held that a federal driver's privacy law prevented a Chicago suburb from issuing tickets that contained the driver's name, address, driver's license number, date of birth, height and weight. The Driver's Privacy Protection Act is a federal law passed after a California actress was murdered by a stalker who obtained personal information from the state department of motor vehicles.

EPIC recently filed a "friend of the court" brief arguing that resellers of state driver records should be strictly liable under the Act. For more information, see EPIC: Driver's Privacy. (Aug. 9, 2012)

- **EPIC Argues That Resellers of State Driver Records Should Be Strictly Liable Under Privacy Law:** EPIC filed a "friend of the court" brief in Gordon v. Softech Int'l, Inc., a case concerning privacy protections for driver records. The Driver's Privacy Protection Act is intended to prevent the misuse of personal information disclosed by state departments of motor vehicles. The Act allows the disclosure of driver record information only for "permissible uses." Some companies resell this information to others. EPIC argued in its brief that when the buyer uses this information for an impermissible purpose, the seller should be liable under the law. Strict liability, EPIC said, is necessary to incentivize resellers to limit the sale of personal information and prevent abuse. For more information, see EPIC: Gordon v. Softech International, Inc. and EPIC: Driver's Privacy. (Jun. 20, 2012)
- **Court: FL Drivers Can Recover for Sale of Personal Data.** The 11th Circuit Court of Appeals has reversed (PDF) a lower court and held that individuals suing to recover for violations under the Drivers Privacy Protection Act do not need to demonstrate actual harm in order to recover monetary damages. In the case, a Florida man sued Fidelity Bank for obtaining the personal information of 565,000 individuals from the State's motor vehicle databases for junk mail purposes. EPIC's brief in the case argued that monetary damages were necessary in order to deter unaccountable data brokers from obtaining personal information from government coffers. For more information, see EPIC's Kehoe v. Fidelity and Doe v. Chao Pages. (Aug. 26, 2005)
- **EPIC Files Brief Supporting Driver Privacy.** EPIC, joined by the American Civil Liberties Union of Florida, has submitted an amicus brief in Kehoe v. Fidelity Bank, a case under the federal Drivers Privacy Protection Act where a bank purchased over 500,000 motor vehicle records from Florida for junk mail solicitations. The brief argues that individuals are entitled to damages under the law when businesses or data brokers intentionally access motor vehicle information. For more information, see EPIC's Kehoe v. Fidelity Page. (Sept. 1, 2004)

Introduction

The Drivers Privacy Protection Act (DPPA), Public Law No. 103-322 codified as amended by Public Law 106-69, was originally enacted in 1994 to protect the privacy of personal information assembled by State Department of Motor Vehicles (DMVs).

The DPPA prohibits the release or use by any State DMV (or any officer, employee, or contractor thereof) of personal information about an individual obtained by the department in connection with a motor vehicle record. It sets penalties for violations and makes violators liable on a civil action to the individual to whom the released information pertains.

The latest amendment to the DPPA requires states to get permission from individuals before their personal motor vehicle record may be sold or released to third-party marketers.

- 18 U.S.C. § 2721 Text of the Drivers Privacy Protection Act of 1994.
- 18 U.S.C. § 2722 Additional Unlawful Acts.
- 18 U.S.C. § 2723 Penalties.
- 18 U.S.C. § 2724 Civil Action.
- 18 U.S.C. § 2725 Definitions.
- Commentary on the DPPA Cornell Legal Information Institute.

History of the DPPA

The DPPA was passed in reaction to the a series of abuses of drivers' personal information held by government. The 1989 death of actress Rebecca Schaeffer was a prominent example of such abuse. In that case, a private investigator, hired by an obsessed fan, was able to obtain Rebecca Schaeffer's address through her California motor vehicle record. The fan used her address information to stalk and to kill her. Other incidents cited by Congress included a ring of Iowa home robbers who targeted victims by writing down the license plates of expensive cars and obtaining home address information from the State's department of motor vehicles.

Senator Barbara Boxer, who sponsored 103 S. 1589, a version of the DPPA, cited other examples where stalkers were able to find victims by simply visiting a DMV. She argued that in "34 States, someone [could] walk into a State Motor Vehicle Department with your license plate number and a few dollars and walk out with your name and home address." Senator Boxer also said:

"In Tempe, AZ, a woman was murdered by a man who had obtained her home address from that State's DMV.

And, in California, a 31-year-old man copied down the license plate numbers of five women in their early twenties, obtained their home address from the DMV and then sent them threatening letters at home. I want to briefly read from two of those letters.

I'm lonely and so I thought of you. I'll give you one week to respond or I will come looking for you.

Another one read:

I looked for you though all I knew about you was your license plate. Now I know more and yet nothing. I know you're a Libra, but I don't know what it's like to smell your hair while I'm kissing your neck and holding you in my arms.

When they apprehended him, they found in his possession a book entitled `You Can Find Anyone' which spelled out how to do just that using someone's license plate.

Senator Chuck Robb also spoke in favor of the DPPA:

"The right to privacy, without which the Americans are not secure in their own homes, is seriously threatened. It is easy for anyone anywhere to access information as personal as your address and phone number, even if they are not listed in the telephone directory. Even your Social Security number is available, and the chief agent giving out this kind of information is the very government that is supposed to protect its citizens.

Many Americans are infuriated and, more importantly, they are vulnerable to these violations of privacy which happen in 34 States in this country every day, my own included.

Recently, a woman in Virginia was shocked to discover black balloons and antiabortion literature on her doorstep days after she had visited a health clinic that performs abortions. Apparently, someone used her license plate number to track down personal information which was used to stalk her.

In another case in Georgia, an obsessive fan obtained the home address of a fashion model from the State Department of Motor Vehicles and assaulted her in front of her apartment.

These are but two examples of how simple it is to submit a driver's license number, pay a nominal fee to the DMV and receive a person's name and address. This is no mere loophole in a system, it is a visible gap that needs to be plugged.

Senator Harkin also spoke favorably of the DPPA, noting that:

"The Drivers Privacy Protection Act, of which I am an original cosponsor, strikes a fair balance between reasonable interests of the State and the public in this information, and the rights of private citizens to be left alone.

I became aware of this issue through the plight of one of my constituents, Karen Stewart. Karen was a patient of Dr. Herbert Remer, a physician who specializes in obstetrics and gynecological care in the Des Moines area. Because Dr. Remer performs abortions, his clinic has been the site of repeated protests by those who oppose women's right to choose.

But Karen was going to Dr. Remer to save her pregnancy, not to terminate it. She was experiencing complications, and went to Dr. Remer for treatment. Unfortunately, a few days after the visit, Karen suffered a miscarriage.

And then she received the letter. Extremists from Operation Rescue sent a venomous letter apparently intended to traumatize Dr. Remer's patients. The letter spoke of `God's curses for the shedding of innocent blood,' and 'the guilt of having killed one's own child.' They got her name and address from department of transportation records, after they spotted her car parked near Dr. Remer's clinic.

The DPPA ultimately passed as an amendment to 103 H.R. 3355, the Violent Crime Control and Law Enforcement Act of 1994.

- 103 H.R. 3365, the DPPA, as introduced in the House of Representatives by Representative Moran.
- 103 S. 1589, the DPPA, as introduced in the Senate by Senator Boxer.
- 103 H.R. 3355, the Violent Crime Control and Law Enforcement Act of 1994. The DPPA is contained within Title XXX, Section 300001.

In 1999 Congress amended the law to give drivers additional privacy protections. The "Shelby amendment," which took affect June 1, 2000, changed the DPPA to require that states obtain a driver's express consent before releasing any personal information, regardless of whether the request is made for a particular individual's information or in bulk for marketing purposes.

The DPPA survived a Constitutional challenge in *Reno v. Condon*, 528 U.S. 141 (2000). In that case, the state of South Carolina challenged the DPPA arguing that the Act violated principles of federalism. The Supreme Court upheld the constitutionality of the Act as a proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause. EPIC filed an amicus brief in that case that argued in part:

The 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. It restricts the activities of states only to the extent that it concerns the subsequent use or disclosure of the information in a manner unrelated to the original purpose for which the personal information was collected. 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.

The DPPA's Provisions

The Drivers Privacy Protection Act requires all States to protect the privacy of personal information contained in an individual's motor vehicle record. This information includes the driver's name, address, phone number, Social Security Number, driver identification number, photograph, height, weight, gender, age, certain medical or disability information, and in some states, fingerprints. It does not include information concerning a driver's traffic violations, license status or accidents.

The Act has a number of exceptions. A driver's personal information may be obtained from the department of motor vehicles for any federal, state or local agency use in carrying out its functions; for any state, federal or local proceeding if the proceeding involves a motor vehicle; for automobile and driver safety purposes, such as conducting recall of motor vehicles; and for use in market research activities. Ironically, personal data is still available to licensed private investigators.

The Act imposes criminal fines for non-compliance and grants individuals a private right of action including actual and punitive damages, as well as attorneys fees.

Permissible Uses of a Driver's Motor Vehicle Record

The DPPA limits the use of a driver's motor vehicle record to certain purposes. These purposes are defined in 18 U.S.C. § 2721:

- Legitimate government agency functions.
- Use in matters of motor vehicle safety, theft, emissions, product recalls.
- Motor vehicle market research and surveys.
- "Legitimate" business needs in transactions initiated by the individual to verify accuracy of personal information.
- Use in connection with a civil, criminal, administrative or arbitral proceeding.
- Research activities and statistical reports, so long as personal information is not disclosed or used to contact individuals.
- Insurance activities.
- Notice for towed or impounded vehicles.
- Use by licensed investigators or security service.
- Use by private toll transportation facilities.
- In response to requests for individual records if the State has obtained express consent from the individual.
- For bulk marketing distribution if State has obtained express consent from the individual.
- Use by any requestor where the reqestor can show written consent of the individual.
- For any other legitimate State use if it relates to motor vehicle or public safety.

If an individual has not given consent to the release of a motor vehicle record, the DPPA limits sharing of information once it is obtained. Information may only be shared with other approved users only for permitted uses. In addition, records must be kept of each additional disclosure identifying each person or entity that is receiving the disclosure and for what purpose. The disclosure records must be kept for a period of 5 years.

State Protections May Be Broader than the DPPA

The DPPA, like many other privacy statutes, provides a federal baseline of protections for individuals. The DPPA is only partially preemptive, meaning that except in a few narrow circumstances, state legislatures may pass laws to supplement the protections made by the DPPA.

States were required to comply with the minimum requirements of the DPPA by September 1997. Many states are more restrictive than the federal rules. Certain states, such as Arkansas and Wyoming, only release personal information to the licensee; a person who has written permission from a licensee; or a traffic court, law enforcement, or governmental agency who has a need for such information to perform their required duties.

States differ as to whether the DPPA applies to records of vehicles owned by corporations, proprietorships, partnerships, limited liability partnerships, associations, estates, lienholders, or trusts.

News

- Welcome to the Database Lounge, The New York Times, March 21, 2002.
- ACLU Urges Congress to Strengthen Drivers' Privacy Protections, ACLU Press Release, April 4, 2000.
- Unanimous Supreme Court Upholds Driver's Privacy Protection Act, Newswatch, February 2000.
- U.S. Supreme Court takes up driver's license data privacy, CNN, May 21, 1999.

Cases

- *Reno v. Condon*, 528 U.S. 141 (2000). In *Condon*, the Supreme Court upheld the constitutionality of the Drivers Privacy Protection Act following a challenge by the state of South Carolina which alleged that the Act violated principles of federalism. The Court held that the Act is a proper exercise of Congress' authority to regulate interstate commerce under the Commerce Clause. Read EPIC's amicus brief that was filed in this case (PDF).
- *Davis v. Freedom of Information Commission*, 259 Conn. 45 (2001). In *Davis*, the Connecticut Supreme Court ruled that the DPPA does not apply to other government agencies who receive personal information from the State DMV in the course of their normal government functions. Therefore, records compiled by the office of the tax accessor, which were based on state motor vehicle records, were publicly accessible.

Resources

- Testimony of Greg Nojeim, Deputy Director of the ACLU on the DPPA, April 4, 2000. ACLU Senate testimony on problems with the DPPA.
- *Comment: Reno v. Condon: The Supreme Court Takes a Right Turn in its Tenth Amendment Jurisprudence by Upholding the Constitutionality of the Driver's Privacy Protection Act*, 68 Fordham L. Rev. 2543, (2000).
- *The Constitutionality of the Driver's Privacy Protection Act: A Fork in the Information Access Road*, 52 Fed. Comm. L.J. 125 (1999). (PDF)
- *Current Development in the Law: A Survey of Federal Cases Involving the Constitutionality of the Driver's Privacy Protection Act*, 8 B.U. Pub. Int. L.J. 555 (1999).

Previous Top News

- **Supreme Court Upholds Drivers' Privacy Law.** The Supreme Court issued its decision in Condon v. Reno, a case concerning the constitutionality of the 1994 Drivers' Privacy Protection Act (DPPA) -- a

federal law protecting personal information collected by state DMVs. In the unanimous decision, the court found that the law does not impinge on states' rights. On July 15, EPIC filed an amicus brief [PDF] in the case arguing that Congress is entitled to protect personal information held by state agencies. (Jan. 12, 2000)

- **Supreme Court Hears Case on Drivers' Records Privacy.** Oral arguments in Reno v. Condon -- a case on the constitutionality of federal regulation over the distribution of information contained within state driving records -- were heard by the Supreme Court. EPIC's amicus "friend of the court" brief [PDF] argued that the 1994 Drivers Privacy Protection Act is a proper exercise of federal legislative authority. (Nov. 10, 1999)
- **Bill Protecting Driver's License Information Sent to White House.** The Department of Transportation and Related Agencies Appropriations Act 2000, in an amendment offered by Sen. Richard Shelby (R-AL), provides two new protections for driver's license information. The first repeals an earlier law requiring Social Security numbers to be displayed on all driver's licenses. The second provision in the amendment takes away federal funding in this bill for states that do not obtain a driver's permission before selling their information to third parties. More information about the privacy risks associated with Social Security numbers and their inclusion on driver's licenses is available from EPIC. The bill has passed Congress and is currently waiting the President's approval. (Oct. 5, 1999)
- **New Documents Reveal Secret Service Role in National Identity Database.** As reported in Wired News, Image Data -- a company seeking to provide a new method of stopping credit card and check fraud -- has been building a database of cross-referenced photographs and purchase histories. Documents obtained by EPIC through Freedom of Information Act requests show the role of the Secret Service in directing and funding Image Data's pilot programs. In its project of establishing an unprecedented national identity database, Image Data purchases driver's license photos without the permission or knowledge of citizens. (Sept. 7, 1999)
- **EPIC Files Brief in Drivers Privacy Case.** The Electronic Privacy Information Center filed an amicus brief [PDF] in the U.S. Supreme Court, arguing that the 1994 Drivers Privacy Protection Act is a Constitutional exercise of Congressional authority. EPIC urged the high court to reverse a lower court opinion which held that the DPPA violated the Tenth Amendment. (July 15, 1999)

Support EPIC

Search epic.org

Hot Policy Issues

- Administrative Procedure Act Comments
- Automobile Event Data Recorders (Black Boxes) and Privacy
- Body Scanners
- Cloud Computing
- Childrens' Online Privacy

- Cybersecurity
- DHS Media Monitoring
- Drones and UAVs
- EU Data Protection Directive
- Facebook
- Facebook Facial Recognition
- FAST Project
- FBI Watchlist
- FCC Google Street View Investigation
- FISA
-
- Fusion Centers
- Google Street View
- Intelligence Oversight Board
- Locational Privacy
- Medical Record Privacy
- National ID
- NSTIC
- Open Government
- PATRIOT Act
- Privacy Convention
- Re-identification
- Search Engine Privacy
- Secure Communities
- Smart Grid
- Social Networking Privacy
- Student Privacy
- Voter Photo ID

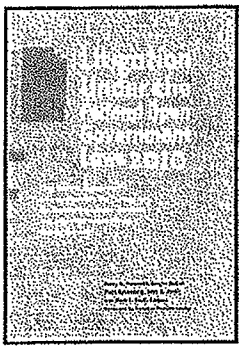
Connect with EPIC

 EPIC on Facebook

 EPIC on Twitter

 EPIC RSS Feed

EPIC Bookstore



Litigation Under the Federal Open Government Laws 2010

More EPIC Publications...