



1999

COMMENTARY: State Sale of Driver's License Data Sparks Debate over Federal Privacy Law

Steven C. Carlson

Follow this and additional works at: <https://digitalcommons.law.yale.edu/yjolt>

 Part of the [Computer Law Commons](#), [Intellectual Property Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Steven C. Carlson, *COMMENTARY: State Sale of Driver's License Data Sparks Debate over Federal Privacy Law*, 1 YALE J.L. & TECH (1999).

Available at: <https://digitalcommons.law.yale.edu/yjolt/vol1/iss1/5>

This Article is brought to you for free and open access by Yale Law School Legal Scholarship Repository. It has been accepted for inclusion in Yale Journal of Law and Technology by an authorized editor of Yale Law School Legal Scholarship Repository. For more information, please contact julian.aiken@yale.edu.

COMMENTARY: State Sale of Driver's License Data Sparks Debate over Federal Privacy Law

Steven C. Carlson*

I. INTRODUCTION

The proliferation of computerized databases of personal information has brought renewed attention to federal privacy law. While privacy rights under the Constitution have traditionally been limited to intimate details of personal lives, recent disputes have raised the question as to whether notions of substantive due process also extend to personal data. The focus of recent disputes has been the practice that thirty-four state motor vehicle departments have of selling the personal data of registered drivers to direct marketing companies and to other firms and individuals.¹

These state agency practices came to light in the wake of serious crimes facilitated by state disclosure of personal data. In 1989, actress Rebecca Schaeffer was murdered when a lunatic fan acquired her address through the motor vehicle records held by the State of California, and shot her.² A federal law, the Driver's Privacy Protection Act (DPPA), was enacted in 1994 to prevent the perceived abuses of state management of driver's license data.³ The Act created a general prohibition on the disclosure of the data,⁴ with enumerated exceptions.⁵ The Act sparked controversy between the federal and state governments upon assertions that Congress lacked constitutional authority for its enactment.⁶

Data privacy law is ripe for review by federal courts. Recent case law, however, has withheld pronouncements on federal privacy rights in favor of resolving disputes according to more traditional doctrines of federalism. Three federal circuit courts of appeals have heard challenges to the DPPA. The cases, bringing to the bench novel issues of privacy law, have been resolved largely under the Commerce Clause. The cases leave open the question of how broadly in scope federal constitutional protection applies to personal data.

* J.D., Yale Law School, 1999; B.A., Chemistry, Reed College, 1993.

¹ See *Condon v. Reno*, 155 F.3d 453, 456 (4th Cir. 1998). Wisconsin, for example, collected approximately \$ 8 million in annual revenues from the sale of driver's license data. See *Travis v. Reno*, 163 F.3d 1000, 1002 (7th Cir. 1998).

² See W. Kent Davis, *Drivers' Licenses: Comply with the Provisions of the Federal Driver's Privacy Protection Act; Provide Strict Guidelines for the Release of Personal Information from Drivers' Licenses and Other Records of the Department of Public Safety*, 14 GA. ST. U. L. REV. 196, 196 (1997).

³ 18 U.S.C. § 2721 (1994).

⁴ See 18 U.S.C. § 2721(a) (1994) ("Except as provided in subsection (b), a State department of motor vehicles, and any officer, employee, or contractor, thereof, shall not knowingly disclose or otherwise make available to any person or entity personal information about any individual obtained by the department in connection with a motor vehicle record.").

⁵ See 18 U.S.C. § 2721(b) (1994) (exempting from the prohibitions of the DPPA disclosures of driver's license data to parties such as: other governmental agencies and law enforcement officials; those involved with motor vehicle safety and theft; businesses for attempting to verify data originally submitted by the individual; and bulk marketers who permit individuals to opt out of inclusion).

⁶ See *Condon*, 155 F.3d at 453; *Travis*, 163 F.3d at 1000; *Oklahoma Department of Public Safety v. United States*, 161 F.3d 1266, 1272-73 (10th Cir. 1998).

Circuit courts have split on the constitutionality of the DPPA. In September 1998, the Fourth Circuit struck down the DPPA as unconstitutional, ruling that Congress lacked authority for its passage under either the Commerce Clause or the Fourteenth Amendment.⁷ In December 1998, the Seventh⁸ and Tenth Circuits⁹ upheld the DPPA, finding that Congress had authority under the Commerce Clause to pass it. These courts did not reach the question as to whether Congress had authority to enact the DPPA pursuant to the Fourteenth Amendment.

ISSUES OF FEDERALISM

The debate over the constitutionality of the DPPA has focused primarily on issues of federalism. Courts have split on the question of whether Congress has power under the Commerce Clause to enact the DPPA.¹⁰ In *Condon v. Reno*, the Fourth Circuit struck down the DPPA and held that Congress improperly regulated the states when it enacted the DPPA. The court based its argument on the premise that Congress is forbidden from regulating “States as States.”¹¹ The Fourth Circuit reasoned that Congress is limited to regulating the activities of states through “legislation that is also applicable to private parties,”¹² repeatedly citing *Garcia v. San Antonio Metropolitan Transit Authority*¹³ to assert that “Congress may only ‘subject state governments to generally applicable laws.’”¹⁴ The Fourth Circuit noted that the DPPA targeted only the practices of state agencies, and had no application to private parties. The court concluded that the DPPA bore unconstitutionally on state governments.¹⁵

The Seventh and Tenth Circuits roundly criticized *Condon*. Congress is free, the courts argued, to regulate the activities of the states, so long as Congress does not attempt to commandeer the legislative processes of the states.¹⁶ Congress is not limited, the courts continued, to regulating the states only through generally applicable laws, as the Fourth Circuit had urged. Laws may be enacted that fall exclusively on the states, especially when similar laws already regulate the conduct of private parties. Privacy law is a prime example. A litany of laws has long regulated private handling of data.¹⁷ Although the DPPA bears solely on states, it is merely a continuation of an existing scheme of regulation that applies to private and public entities alike.¹⁸ Nor does the DPPA commandeer the administrative processes of the states, the courts argued. Although the states must train personnel to comply with federal law, this does not constitute “commandeering,” as articulated in *New York v.*

⁷ See *Condon*, 155 F.3d at 463, 465.

⁸ See *Travis*, 163 F.3d at 1001-02.

⁹ See *Oklahoma*, 161 F.3d at 1272-73.

¹⁰ See *Condon*, 155 F.3d at 460-463.

¹¹ See *Condon*, 155 F.3d at 458.

¹² See *Condon*, 155 F.3d at 461.

¹³ 469 U.S. 528 (1985).

¹⁴ See *Condon*, 155 F.3d at 461 (emphasis added).

¹⁵ See *Condon*, 155 F.3d at 463.

¹⁶ See *Travis*, 163 F.3d at 1003; *Oklahoma*, 161 F.3d at 1269-70.

¹⁷ See *Travis*, 163 F.3d at 1005.

¹⁸ See *id.*

United States.¹⁹ Under this argument, the Seventh and Tenth Circuits concluded that Congress had properly passed the DPPA pursuant to its powers under the Commerce Clause.²⁰

PRIVACY ISSUES

The DPPA raises novel questions of privacy law that were largely sidestepped by the courts. Arguably, the DPPA is justified by the Enforcement Clause of the Fourteenth Amendment.²¹ The Court has recognized that substantive due process implies a federal right to privacy that may not be abridged by the actions of state government.²² The federal right to privacy has been most firmly established in the area of reproductive rights.²³ The Fourteenth Amendment also ensures the privacy of personal data. The question of what types of data fall under the protections of the federal Constitution is the issue that underlies DPPA litigation.

Privacy rights in personal data have been litigated in two primary contexts. First, courts have upheld the right of government agencies to acquire personal data from private sources, when such compulsory disclosure advances legitimate public interests. State departments of health, for example, may compel physicians to disclose medical records of patients who take potentially addictive drugs.²⁴ Similarly, the National Institute for Occupational Safety and Health was found to have a valid interest in compelling private companies to disclose medical records of workers exposed to work-related hazards.²⁵

Second, courts have prohibited the release of certain types of personal information by the state to the general public. Courts recognize that information falls under the protection of the federal Constitution when the individual has a "legitimate expectation . . . that [the information] will remain confidential while in the state's possession."²⁶ Courts balance the interests of individuals in suppressing the disclosure of confidential information with the interests of the state in advancing policy goals.²⁷ For example, no compelling state interest was found to justify a sheriff's disclosure to the press of embarrassing details of a rape.²⁸ Also, a state was found to have unjustifiably abridged

¹⁹ See *Travis*, 1998 163 F.3d at 1003-05 (citing *New York v. United States*, 505 U.S. 144 (1992)); *Oklahoma*, 161 F.3d at 1271-72.

²⁰ See *Travis*, 161 F.3d at 1001-02; *Oklahoma*, 161 F.3d at 1772-73.

²¹ The Fourteenth Amendment provides, in pertinent part, that:

§ 1. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States;

nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any persons within its jurisdiction

the equal protection of the laws.

. . . .

§ 5. The Congress shall have power to enforce, by appropriate legislation, the provisions of this article.
U.S. CONST. amend. XIV, §§ 1, 5.

²² See *Roe v. Wade*, 410 U.S. 113 (1973).

²³ See *Griswold v. Connecticut*, 381 U.S. 479 (1965); *Wade*, 410 U.S. 113.

²⁴ See *Whalen v. Roe*, 429 U.S. 589 (1977).

²⁵ See *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570 (3d Cir. 1980).

²⁶ *Mangels v. Pena*, 789 F.2d 836, 839 (10th Cir. 1986).

²⁷ See *Bloch v. Ribar*, 156 F.3d 673, 686 (6th Cir. 1998).

²⁸ See *id.*

the legitimate expectations of a murder suspect by releasing the diary of his slain wife to novelists.²⁹ Medical records are afforded a similar degree of confidentiality.³⁰

The bounds of the federal right to privacy are undefined.³¹ The Fourth Circuit has held, however, that driver's license data falls outside the protections of the Fourteenth Amendment. The court noted that the information contained in drivers' licenses is widely available from other sources, and that the information is routinely given to strangers. "The information found in motor vehicle records is not the sort of information to which individuals have a reasonable expectation of privacy," the Fourth Circuit concluded.³² The Seventh and Tenth Circuits have remained silent on the topic.

The holding of the Fourth Circuit is consistent with a general reluctance in the judiciary to extend the scope of constitutional privacy law beyond information about individuals' intimate details.³³ *Condon*, however, is silent as to whether people, such as murdered actress Rebecca Schaeffer, might have a "legitimate expectation" that state agencies will refrain from disclosing personal information to unknown inquisitors, or from selling personal data to direct marketing firms. Nor did the Fourth Circuit consider whether states advance viable policy goals through the lucrative practice of data dissemination. If driver's license data does not trigger the protections afforded by the Fourteenth Amendment, then it is not clear whether constitutional protections should extend to other forms of state-held data, such as Social Security numbers and tax records.

States are in the process of revamping their data management systems.³⁴ They are consolidating the databases of their various agencies, and are privatizing the maintenance of their systems.³⁵ As data becomes more readily available, privacy law will become even more critical. Information that is available from other sources, or that may be routinely shared with strangers, will soon be aggregated in centralized databases. As the accessibility of personal data grows, so does the "legitimate expectation" of confidentiality and the need for a rational privacy doctrine.

²⁹ See *Sheets v. Salt Lake County*, 45 F.3d 1383, 1387-89 (10th Cir. 1995).

³⁰ See *Whalen*, 429 U.S. at 589.

³¹ See *Eagle v. Morgan*, 88 F.3d 620, 625 (8th Cir. 1996) ("We acknowledge that the exact boundaries of this right are, to say the least, unclear.").

³² *Condon*, 155 F.3d at 465.

³³ See, e.g., *Sheets*, 45 F.3d at 1387.

³⁴ See, e.g., INFORMATION TECHNOLOGY ARCHITECTURE & PLANNING DIVISION, STATE OF CONNECTICUT, STATE OF CONNECTICUT STRATEGIC PLAN FOR INFORMATION TECHNOLOGY (1998), available at <<http://www.doit.state.ct.us/StrategicPlan.htm>>.

³⁵ See *id.* ch. 3(1).